Certificate Practice Statement

for the

Navy Acquisition Public Key Infrastructure

Version 2.0

Charlene F. Tallman 10·21·99

Charlene F. Tallman
Information Systems Security Manager, NAVSUP

Prepared by Operational Research Consultants

TABLE OF CONTENTS

1 SCOPE

1.1 PURPOSE

This Navy Acquisition Certification Practice Statement (CPS) represents the policy and practices for maintaining the Navy Acquisition Public Key Infrastructure (NA PKI); the requirements for other Certificate Authorities (CAs) to be cross-certified with this PKI at any level; the practices for implementing CAs in this infrastructure; and the policies and procedures relating to holding or using certificates issued by these CAs. This CPS is applicable to all agencies and individuals who will be interacting with the NA PKI including DoD activities, other government agencies, associated contractors, and vendors.

This CPS is written to conform with the draft DoD Certificate Policy (CP). The CP takes precedence in any policy discrepancies. The CPS takes precedence in operational discrepencies.

1.2 APPLICATION

1.2.1 Audience

This CPS is applicable to all agencies and individuals who will be interacting with the NA PKI, including Navy activities, other government agencies, contractors, foreign nationals, and organizations. The obligations and policies in this CPS also apply to applications and servers that rely on certificates issued under the NA PKI.

1.2.2 Time Period

This CPS and resulting PKI is effective as an on-going Navy approved pilot to provide functionality supplemental to the Depatment of Defense (DoD) Medium Assurance Pilot PKI. As functionality becomes available within the DoD PKI, subscribers and relying parties of the NA PKI will be migrated to the DoD PKI. It is anticipated that as the target DoD PKI becomes operational that the NA PKI pilot will stand down.

1.3 DOCUMENT OVERVIEW

This document is divided into four sections. This first section introduces the document. Section two provides a general introduction to PKI terms and concepts. Section three identifies NA PKI policy and requirements for cross-certifying with CAs within this PKI. Section four describes all processes and procedures to:

- Install, operate and maintain CAs;
- Request, issue, cancel, publish, and revoke certificates;
- Protect the PKI; and
- Verify validity of certificates.

2 OVERVIEW

2.1 BACKGROUND

2.1.1 Introduction

The commercial sector is rapidly adopting public key encryption solutions that provide security services. The Internet Engineering Task Force (IETF) has established a working group, which has published standards for implementing public key infrastructures. Major software vendors, including Netscape, Microsoft, and Lotus have moved towards incorporating these standards into their products, and third-party solutions are available. With this commercial support, securing information in transit is becoming a reachable goal.

The Computer Security Act of 1987 defines the requirements for Sensitive But Unclassified (SBU) data and supports the premise that essentially all business conducted within the federal government is SBU. SBU is to be protected in computer systems containing federal government data, including those owned and operated by contractors. This congressional act sanctions National Institute of Standards and Technology (NIST) to define requirements for Automated Information Systems and it establishes these requirements as binding on United States (U.S.) Government agencies. NIST has published a number of Federal Information Processing Standards (FIPS) to outline these requirements. SECNAVINST 5239.3, dated 14 July 1996, enacts policy that protects AIS and data within the Navy.

Industry standard digital certificates play a central role in protecting SBU. Digital certificates are digital documents that vouch for the identity and key ownership of:

- Individuals;
- Computer systems or specific applications running on those systems; and
- Organizations.

In general, personal certificates serve the following purposes:

- Publish a public key for individuals and applications to use to send encrypted messages that can only be read by the certificate owner;
- Certify identity of an authenticate the certificate owner to other individuals or applications; and

- Digitally sign documents and electronic mail messages.

Digital certificates are used in conjunction with cryptographic modules to accomplish encryption. FIPS 140-1, Security Requirements for Cryptographic Modules, sets standards for implementing cryptographic modules. NIST evaluates cryptographic modules for compliance with FIPS 140-1 and publishes a list of validated modules. This list may be viewed at *http://csrc.ncsl.nist.gov/cryptval/140-1/1401val*.htm. The Navy only endorses cryptographic products whose cryptographic modules are certified by NIST as FIPS 140-1 compliant for SBU.

A PKI is dedicated to the management of certificates used by public key enabled applications. PKI services are important in networked environments where communications and transactions occur over unsecured channels. PKI can provide the following services:

- Confidentiality - secure data from individuals who are not authorized to view it;
- Integrity - assure that data has not been modified;
- Identification and Authentication - ensure that only appropriate individuals gain access to computer resources;
- Non-repudiation - prevent individuals from denying actions that actually took place;
- Privilege and Authorization - limit the data available to individuals according to need to know; and
- Key Recovery - restore encryption keys if they become lost or damaged. *[Note: Key Recovery is not supported by the NA PKI at this time.]*

A PKI shall assure the trustworthiness of all components that make up the PKI, including hardware and storage media, and allow scalability. It is important that any PKI is standards based to ensure interoperability with other PKIs. PKI components include Certificate Authority and directory software, policies, procedures, processes, and individuals performing trusted roles which support wide-scale management of keys and certificates.

A CA is used to:

- Issue standard X.509v3 certificates;
- Provide a trusted authority to validate people and computer systems;
- Provide an assurance level; and
- Accomplish chaining and cross-certification with other authorities for interoperability of PKIs. *[Note: NA PKI supports chaining directly and cross-certification indirectly through a combination of server and directory configurations.]*

A directory is a directory that supports the Lightweight Directory Access Protocol (LDAP). Directories provide ready access to certificates and Certificate Revocation Lists (CRLs). Access Control Lists (ACLs) may also be managed from a directory.

Policies, procedures, and processes provide information on a PKI to the subscriber (certificate holder), the relying party (certificate user), and agencies wanting to cross-certify with a CA. These policies, procedures, and processes may be defined in a Certificate Practice Statement, which explains valid usage of certificates, and a Concept of Operations (CONOPS), which illustrates how a PKI functions within the organization.

2.1.2 DoD PKI

The Defense Information Systems Agency (DISA) has implemented a Medium Assurance Pilot PKI in the DoD to protect SBU data. DISA estimates that approximately two million DoD users will have digital certificates within the next two years. This technology can meet a large part of the DoD's requirements to protect sensitive data.

The DoD PKI utilizes industry standard Commercial Off The Shelf (COTS) components incorporating IETF standards, including Public Key Certificate Standards (PKCS). The DoD PKI consists of centralized CA and directory components combined with distributed Registration Authorities (RAs) and Local Registration Authorities (LRAs) who register subscribers.

The DoD PKI focuses on digital signatures for DoD civilian and military employees and contractors who work full time on-site at DoD facilities. DoD PKI applications currently under development include the Defense Travel System (DTS), and the Joint Electronic Commerce Program Office (JECPO) Electronic Document Access (EDA).

2.1.3 Supplemental Navy Acquisition PKI Requirements

The Navy's requirement to protect SBU data is the same as all other government agencies. Because of the extensive partnerships between Navy Systems Commands and private industry, these commands have an immediate need to transmit SBU data through existing electronic networks, including the Internet. Some of the requirements with this immediate need include:

- Cross-certification with industry (contractors) and foreign nationals;
- Issuing certificates to off-site contractors, foreign nationals, and vendors;
- Directory maintained single-sign-on for secure server access;
- Real time revocation status checking; and

· Secure electronic mail with industry.

In order to meet these immediate data transfer requirements and gain knowledge and experience in the implementation and use of a PKI, the Naval Air Systems Command (NAVAIR), the Naval Supply Systems Command (NAVSUP), and the Naval Sea Systems Command (NAVSEA), established the NA PKI. Six months of planning led to initial implementation in August 1997. The NA PKI has been acknowledged by CNO and SPAWAR PMW-161, and has been briefed to the DoD PKI Working Group. The NA PKI has been concentrating on cooperation with prime and support contractors. NAVAIR and NAVSUP are active in the DoD PKI Working Group and are using DoD licensed NIST approved software for protecting SBU. The NA PKI design enables a smooth transition to those functions supported by the DoD PKI as that PKI becomes widely deployed. Since the inception of the NA PKI, it has provided FIPS 140-1 validated encryption solutions for servers and user clients. Commercial CAs are a part of the NA PKI for contractors who do not or will not have initiated a company PKI.

Although the NA PKI is compatible with the DoD PKI, it is supplemental since it goes beyond the DoD PKI initiative in the areas of coordinating with outside organizations (i.e. prime and support contractors). Members of the NA PKI are actively informing the DoD PKI Working Group of requirements as they are discovered. After new required capabilities are implemented at DoD PKI, the NA PKI users will migrate to the DoD PKI.

In accordance with the August 11, 1998 ASD(C3I) memo acknowledging ongoing PKI pilots, participating Navy systems commands have evaluated the costs and risks of the NA PKI and plan to continue operation as a supplement to the DoD PKI. This Certificate Practice Statement governs the NA PKI Root CA and the subordinate CAs. The implementation of PKI technology is supported by on-line and live training packages, as well as a help desk. The NA PKI CAs operate only as a supplement to the DoD PKI by filling in functionality not currently supported or fielded by the DoD. DoD PKI certificates will be used as required functionality is supported. As additional capabilities become functional under the DoD PKI, they will be phased into the operational program offices.

2.2 TERMS AND DEFINITIONS

Certificate Authority - A Certificate Authority (CA) is a system that issues certificates, responds to certificate validation requests, publishes Certificate Revocation Lists (CRLs), and generates audit and archive information. Components of the CA include hardware, CA software, database software, and the Certificate Authority Administrator (CAA).

Certificate Authority Administrator - A Certificate Authority Administrator (CAA) is an individual who is the responsible party for a CA. The CAA possesses the private key of the CA's certificate. The CAA may be colocated with the CA, but may also perform administration tasks remotely.

Certificate Policy – A Certificate Policy (CP) is a document which defines the overall policies for a given PKI.

Certificate Practice Statement - A Certificate Practice Statement (CPS) is a document which details the requirements and procedures that are followed by a CA in issuing and maintaining certificates, and the purposes and allowed uses of those certificates.

Certificate Repository - A certificate repository is a system that holds certificates and information about all unexpired certificates including revocation information.

Certificate Revocation List - A Certificate Revocation List (CRL) is a list of certificates that have been revoked but have not yet expired. A CRL should be digitally signed by the CA to ensure its validity to relying parties.

Cross-Certification - Cross-certification is a process by which two distinct CAs establish a trust relationship with each other. Cross-certified CAs agree that their respective policies and regulations are compatible, and that certificates issued by one CA may be accepted by applications who trust the certificates issued by the other CA.

Digital Certificate - A digital certificate is electronic information that indicates the identity of the subscriber, the identity of the issuing CA, the operational period of the certificate, and the public key of the subscriber. The certificate is digitally signed by the issuing CA to show validity.

Digital Signature – A digital signature is an electronic attachment to a document that can be used to validate the identity of the individual signing the document and attests that the information in the document has not changed since it was signed.

Information Systems Security Manager - An Information Systems Security Manager (ISSM) is the individual at each site with primary responsibility for information systems security at that site.

Information Systems Security Officer - An Information Systems Security Officer (ISSO) is the individual with primary responsibility for the security of a specific information system.

Issuing Authority - An Issuing Authority (IA) is an individual who is responsible for granting certificate requests. There can be multiple IAs for a single CA. IAs can be colocated with the subscribers requesting certificates, but can also issue certificates remotely.

Interim External Certificate Authority – An Interim External Certificate Authority (IECA) is a vendor who has been authorized by the DoD PKI to issue certificates to off-site contractors for a per-certificate fee that can be relied on by approved DoD PKI pilot programs.

Key Escrow - Key escrow is a process for centrally storing individual keys so that they can be restored in the event of loss or damage to the original key.

Key Pair - A key pair consists of a private key and a public key, which can be used asymmetrically to encrypt and decrypt information. Information encrypted using the private key can only be decrypted using the public key, and information encrypted using the public key can only be decrypted using the private key.

Local Registration Authority – A Local Registration Authority (LRA) is an individual performing the trusted role of validating subscriber identity for the DoD PKI. LRAs have limited ability to approve certificate issuance for validated individuals, but cannot revoke certificates or issue server certificates.

Private Key - A private key is the half of a key pair that is kept confidential by the holder. Private keys are used to digitally sign messages and to unencrypt messages that were encrypted with the public key.

Public Key - A public key is the half of a key pair that is publicly available. Public keys are used to validate digital signatures and to encrypt messages that are intended only for the holder of the private key.

Public Key Infrastructure - A Public Key Infrastructure (PKI) is a system of policies, CAs, certificates, information repositories, and trusted individuals, that is used to verify and authenticate individuals and servers, and to encrypt and decrypt information exchanged by these individuals and servers

Registration Authority - A Registration Authority (RA) is an individual who is responsible for verifying the information contained in a subscriber's certificate request. Generally, RAs will be physically colocated with the subscribers that they are verifying. Ideally, the RA would personally know the subscriber.

Relying Party - A relying party is an individual, server, or application that relies on digital certificates to authenticate identity or establish encrypted communication with another individual, server, or application.

Sensitive But Unclassified - Sensitive But Unclassified (SBU) is a data classification within the federal government applied to information that is not designated classified but that is company proprietary or otherwise sensitive and shall be protected in accordance with the Computer Security Act of 1987.

Smart Card – A smart card is a token that follows the International Standards Organization standard 7816 and consists of a chip embedded in a plastic card. The chip contains read-only memory and re-writable memory. A cryptographic smart card is a card which stores a digital certificate within the re-writable memory and performs cryptographic functions within the operating system in the read-only memory.

Subscriber - A subscriber is an individual or a server that has been granted a certificate by a CA. Any server subscriber shall have a designated responsible party, who holds the password to unlock the certificate private key on the server, and who is responsible for ensuring that the server is compliant with all policies and regulations.

System Administrator - A System Administrator (SA) is an individual who has control over the hardware and operating system software on a server. The SA may also have control over database or other application software on the server.

Trusted Agent – A Trusted Agent (TA) is an individual who works directly with an RA to assist in providing face to face identification of subscribers requesting digital certificates. TAs do not receive full RA training and may not submit request validations directly to the IA.

3 POLICY

3.1 SENSITIVE BUT UNCLASSIFIED DATA

In accordance with Federal Law, the DoD Web Policy, and Navy policy, SBU data shall be protected in transit. The NA PKI meets the authentication and encryption requirements of SBU data. Servers, individuals, and applications that handle SBU data use certificates generated under this PKI to meet the SBU protection requirements.

SBU data includes, but is not limited to, the following types of information:

- **Proprietary Data** - Trade secrets and commercial or financial information;
- **For Official Use Only** - Categories of information exempt from public release under the provisions of the Freedom of Information Act (FOIA);
- **Treaties and International Agreements** - Information which shall be protected in accordance with the stipulations of a particular treaty or international agreement such as the Chemical Weapons Compliance Treaty or the North American Free Trade Agreement;
- **Technical Military Data** - Technical data with military or space application which may not be exported lawfully outside the U.S. without prior approval, authorization, or license under the export act of 1979 or the Arms Export Control Act;
- **Export Control Data** - Data which is subject to export controls (international traffic in arms regulation, export control act, U.S. munitions list);
- **Competition Sensitive Data** - Data associated with ongoing procurement of government supplies, services or equipment to include contractor bids and proposals and associated government documents;
- **Privacy Act** - Information which shall be protected from public release to protect the privacy of the individual (social security number, investigative data, payroll records, disciplinary records, etc.);
- **Investigative and Inquiry Data** - Information associated with or resulting from criminal, civil, security, inspector general, flight safety, or other investigations or inquiries which shall be protected from public release; and
- **Naval Nuclear Propulsion Information** - Information concerning the design and operation of Naval nuclear reactors and associated equipment which does not meet the criteria for classification under Executive Order 12958.

3.2 PKI ASSURANCE LEVEL

The draft DoD PKI Roadmap defines four assurance levels for certificates. DoD Class 2 is intended for applications handling information of low value (Unclassified) and does not require that the end user register in person and their cryptography can be software based. DoD Class 3 is intended for applications handling medium value information in a low to medium risk environment and requires in-person registration. DoD Class 4 is intended for applications handling medium to high value information in any environment and requires in-person registration and hardware based cryptographic tokens. DoD Class 5 is intended for applications handling classified information in a high-risk environment and requires NSA approved Type I cryptography.

NA PKI certificates are intended to be equivalent to the DoD Class 3 assurance level. These certificates can be used to:

- Verify the identity of electronic mail correspondents;
- Encrypt the contents of electronic mail messages *[NOTE: NA PKI certificate private keys are not escrowed. For the scope of this pilot, this capability is not applicable.]*;
- Verify the identity of web servers;
- Verify the identity of individuals accessing data servers;
- Verify the integrity of software and documents posted on data servers;
- Encrypt the contents of data transfers between individuals and data servers; and
- Provide a digital signature capability.

NA PKI certificates are acceptable for use with data categorized up to and including Sensitive But Unclassified.

NA PKI certificates are not approved for processing classified information.

3.3 PARTICIPANTS

3.3.1 Navy Acquisition Commands

Employees of participating Navy Systems Commands are subject to the requirements and policies of this CPS as implemented by their local command.

3.3.2 Other Government Employees

Employees of government agencies who do not currently have the ability to receive certificates from their own organization but require certificate authentication to access Navy System Command resources, may request individual or server certificates under the NA PKI. They are subject to the requirements and policies of this CPS as implemented by the command hosting the resource.

3.3.3 Contractor Personnel

Contractor personnel, who have a requirement to access government information or services that are a part of the NA PKI, may participate in the PKI and may request individual or server certificates. Contractors who have certificates issued under this PKI shall be subject to all requirements of this CPS. Certificates issued to contractor personnel shall clearly show that the certificate holder is a contractor employee.

Contractor personnel who are authorized to participate in trusted roles within this PKI shall also be subject to requirements listed in section 4.5.3.7.

3.3.4 Foreign Nationals

Foreign nationals who have a requirement to access government information or services that are a part of the NA PKI may participate in the PKI and may request individual certificates pending legal guidance on export laws of cryptographic information. Foreign nationals who have certificates issued under this PKI shall be subject to all requirements of this CPS. Certificates issued to foreign nationals shall clearly show that the certificate holder is a foreign national and state the country of citizenship.

3.3.5 Organizations

Organizations who wish to do business with government agencies that require NA PKI certificates for access may participate in the PKI and may request individual certificates. Organizations who have certificates issued under this PKI shall be subject to all requirements of this CPS. Certificates issued to organizations for this purpose shall clearly indicate that the certificate is to identify the organization or a designated individual within the organization and shall state the name of the organization. It is preferred that certificates are issued to individuals rather than to organizations.

3.3.6 Cross-Certified CAs

Companies or government organizations that wish to stand up their own PKIs may cross-certify with the NA PKI at any level. All cross-certification requirements as specified in this CPS shall be met. Individuals holding certificates issued by cross-certified PKIs shall be subject to all requirements listed in this CPS and any local policies in effect.

3.3.7 Applications and Servers

Applications run by or in support of participating Navy Systems Commands may participate in the NA PKI and may request server certificates. Applications may also rely on individual certificates issued under this PKI for identification and authorization. Requests for server certificates shall include name, phone number, and email address of a designated point of contact for that server. Application owners and operators are subject to the requirements and policies of this CPS as implemented by the command hosting the resource.

4 PRACTICES

4.1 INTRODUCTION

4.1.1 Overview

This CPS is the policy and implementing document for the NA PKI, which includes all Certificate Authorities (CAs) that share the Navy Acquisition root. In addition, it serves as a guideline for external agencies wishing to cross-certify with any CA in this PKI. This CPS applies to government and non-government subscribers holding certificates issued by any CA in the NA PKI including:

- Contractor personnel requiring access to government resources;
- Servers owned and operated by contractors that are used in support of Navy contracts;
- Foreign nationals requiring access to government resources; and
- Organizations desiring to do business with government agencies.

Government-issued certificates shall be used only for allowing approved access to government applications and data. By accepting a government-issued certificate, individuals accept the obligation to inform the government of any changes in job responsibilities that affect their right to hold a certificate.

This CPS applies to medium assurance certificates and will be used to protect information up to and including SBU. The policies and procedures in this CPS are applicable to individuals who directly use these certificates, and individuals who are responsible for applications or servers that use certificates. Certificate users include, but are not limited to, CAs, IAs, Registration Authorities (RAs), Trusted Agents (TAs), subscribers, and relying parties.

4.1.2 Identification

The Object Identifier (OID) for the NA PKI is unregistered with an identification of: Id-NAVY-acq-medium-pilot.

4.1.3 Community and Applicability

4.1.3.1 Certification Authorities

The NA PKI uses a hierarchical certificate authority structure for identification purposes and to minimize risk in the event of a compromise of trust on any single CA. CAs within this hierarchy have a standard tree relationship, with the root of the tree being self-signed, and signing the certificates of its child CAs. The signing CA is considered the parent CA.

The Acquisition Root CA is the apex of the PKI hierarchy. The Acquisition Root certificate is the ultimate source of authenticity for all certificates created within its domain. This certificate provides the foundation on which all subordinate certificates are built. The Acquisition Root certificate is possessed by every PKI client, and is referred to during the process of validating subject certificate paths. The Acquisition Root CA signs certificates only for second level CAs that are managed by a specific command.

The second tier of CAs within the NA PKI represent the different commands that participate in the PKI. These CAs sign certificates only for the third-tier CAs within that command's jurisdiction.

The third tier of CAs are used to issue certificates. They are determined by the desire of the command to segregate CA activities. CAs are generally broken out geographically or functionally. Different subscriber types are also segregated by which CA at this level issues their certificates. These CAs are responsible for authenticating and registering users, creating certificates, transmitting certificates to the directory, and managing keys and certificates.

4.1.3.2 Agents

4.1.3.2.1 Issuing Authorities

Only Navy employees or their designated representatives will be authorized to issue certificates under this PKI. Issuing Authorities (IAs) may be military, civilian, or contractors. Designation of IAs will be determined at each CA site in accordance with the existing site organizational policies and the requirements of this CPS. IAs shall be issued IA certificates stored on hardware tokens for the purpose of issuing validated certificates to applicants. IAs shall appear in person to the CAA for identity verification with an official photo ID. IAs shall be provided training in issuing certificates and in the policies and processes of this CPS prior to being issued IA certificates. IA duties shall be a primary job responsibility for those individuals.

4.1.3.2.2 Registration Authorities

Only Navy employees or their designated representatives will be authorized to verify certificate requests under this PKI. Registration Authorities (RAs) may be military, civilian, or contractors. Designation of RAs will be determined at each system command in accordance with existing site organizational policies and the requirements of this CPS. RA duties will likely be a secondary job function for RAs. RAs shall be provided training in identity proofing and in the policies and processes of this CPS prior to taking on RA duties.

4.1.3.2.3 Trusted Agents

Only Navy employees or their designated representatives will be authorized to act as trusted agents to perform face-to-face validation for RAs under this PKI. Trusted Agents (TAs) may be military, civilian, or contractors. Designation of TAs is at the discretion the primary RA for the command. TA duties will be a secondary job function for TAs. TAs shall be provided training in identity proofing and supporting the RA responsibilities prior to taking on TA duties.

4.1.3.3 End Entities

4.1.3.3.1 Subscribers

Subscribers are limited to Navy personnel, Navy-owned servers, contractors requiring access to government resources, servers owned by contractors which are used in support of Navy contracts, foreign nationals requiring access to government resources, and organizations seeking to do business with government agencies. Certificates shall clearly state whether the subscriber is government, contractor, foreign national, or an organization representative.

4.1.3.3.2 Relying Parties

Navy Acquisition certificates may be used by any relying party in accordance with the limitations on the use of these certificates as specified in this CPS.

4.1.3.4 Applicability

4.1.3.4.1 Suitable Applications / Protocols

The certificates issued under this PKI are suitable for:

- Verifying the identity of individuals using web server access and applications such as electronic mail;
- Verifying the identity of web servers to individuals;

- Encrypting electronic mail;
- Verifying the integrity of software and documents that are posted on web servers; and
- Non-repudiation for financial or electronic commerce applications.

Various application protocols are acceptable, including Secure Multipurpose Internet Mail Extensions (S/MIME), Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS), and Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS).

4.1.3.4.2 Restricted Applications

No stipulation.

4.1.3.4.3 Prohibited Applications

Any application which does not follow approved standards for the storage and transmittal of cryptographic information is prohibited. Applicable standards include:

- ITU X.509 Version 3
- FIPS 140-1, Security Requirements for Cryptographic Modules;
- FIPS 180-1, Secure Hash Algorithm;
- FIPS 186, Digital Signature Algorithm
- PKCS #11 Hardware Format; and
- PKCS #12 Software Format.

4.1.4 Contact Details

4.1.4.1 Specification Administration Organization

The NA PKI Working Group (WG) is responsible for registration, maintenance, and interpretation of this CPS. The Lead is Ms. Charlene Tallman, NAVSUP SUP63D.

4.1.4.2 Policy Contacts

4.1.4.2.1 NAVSUP

Ms. Charlene Tallman, (717) 790-1432, Charlene_F_Tallman@navsup.navy.mil.

4.1.4.2.2 NAVAIR

Mr. Don Traeger, (301) 757-1571 x41, traegerdr@navair.navy.mil.

4.1.4.3 Technical Contact

Mr. Robert Cope, Operational Research Consultants, Inc., (703) 535-5320, coper@orc.com.

Ms. Rebecca Nielsen, Operational Research Consultants, Inc., (703) 535-5340, nielsenr@orc.com.

4.2 GENERAL PROVISIONS

This section contains provisions relating to the obligations of CAs, IAs, RAs, TAs, Subscribers, Relying Parties, and the certificate repository. It also addresses other issues pertaining to law and dispute resolution. These requirements pertain to all CAs within the NA PKI and any approved cross-certified CAs.

4.2.1 Obligations

4.2.1.1 CA Obligations

Each CA within the NA PKI shall meet the following obligations:

- To immediately revoke an IA, RA, or subscriber certificate and inform the certificate holder if private key compromise is suspected *[NOTE: Revoking a certificate causes that certificate to be listed in the CRL in the repository.]*;
- To work with an IA to revoke and reissue subscriber certificates, if necessary, that were issued by that IA if private key compromise of the IA certificate is suspected;
- To inform IAs and the parent CA of any changes in CA status;
- To protect the CA certificate private key from unauthorized access in accordance with section 4.6.2;
- To immediately inform the parent CA if private key compromise of the CA certificate is suspected and determine if CA certificate revocation is necessary *[NOTE: Revoking the CA certificate immediately invalidates all IA, RA, and subscriber certificates issued by that CA.]*;
- To work with child CAs in the event of suspected private key compromise to determine if CA certificate revocation is necessary; and

- To inform parent CA and all child CAs if any CA certificate is revoked.

Each CA accepts the following obligations to relying parties who follow the policies of this CPS:

- The certificate was issued to the named subscriber,
- The information in the certificate is accurate (including, but not limited to the subscriber Distinguished Name in the subject field and the subject public key information field), and
- The subscriber has accepted the certificate.

The each CA also accepts the obligation to maintain records necessary to support requests concerning its operation, including audit files and archives.

4.2.1.2 IA Obligations

When issuing certificates under this CPS, the Issuing Authority (IA) accepts the following obligations:

- Issue certificates only when both the subscriber's request and the RA validation have been received,
- Notify the subscriber through electronic mail or other means that the certificate request has been granted in accordance with section 4.2.6.1,
- Notify a subscriber of certificate revocation in accordance with section 4.2.6.2.

The IA accepts the following obligations associated with holding an IA certificate:

- To use the IA certificate only for purposes associated with the IA function;
- To cancel certificate requests upon notification from the RA that the request is invalid;
- To immediately revoke an RA or subscriber certificate and inform the certificate holder if private key compromise is suspected;
- To work with an RA to revoke and reissue subscriber certificates, if necessary, that were validated by an RA whose private key is suspected to be compromised;
- To inform RA and the CA of any changes in IA status;
- To protect the certificate private key from unauthorized access; and
- To immediately revoke the IA certificate and report to the CA if private key compromise is suspected.

4.2.1.3 RA Obligations

RAs are obligated to accurately represent the information prepared for the NA PKI and to process requests and responses timely and securely. RAs may accept face-to-face validation information from designated TAs, but it is the RAs responsibility to ensure that their trusted agents act within the requirements of this CPS.

When validating subscriber requests for certificates issued under this CPS, a RA accepts the following obligations:

- To validate the accuracy of all information contained in the subscriber's certificate request;
- To validate that the named subscriber actually requested the certificate;
- To verify the identity of a TA providing the validation information;
- To ensure that the TA validation meets the requirements of this CPS for identity validation; and
- To verify to the IA that the certificate request originated from the named subscriber and that the information contained in the certificate request is accurate.

The RA accepts the following obligations associated with holding a RA certificate:

- To use the RA certificate only for purposes associated with the RA function;
- To revoke and verify reissue of a subscriber's certificate upon notification of changes to information contained in the certificate;
- To immediately revoke a subscriber certificate and inform the IA and the subscriber if private key compromise is suspected;
- To inform and the IA of any changes in RA status;
- To protect the certificate private key from unauthorized access; and
- To immediately request revocation of the RA certificate and report to the IA if private key compromise is suspected.

4.2.1.4 TA Obligations

Trusted agents work with RAs to validate identity of subscribers. They do not hold special certificates and are not authorized to submit validations to the IA. Instead, the TA notifies his or her associated RA that an identity validation has taken place and the RA submits the validation to the IA.

When validating subscriber requests for certificates issued under this CPS, a TA accepts the following obligations:

- To validate the accuracy of all information contained in the subscriber's certificate request;
- To validate that the named subscriber actually requested the certificate; and
- To verify to the RA that the certificate request originated from the named subscriber and that the information contained in the certificate request is accurate.

4.2.1.5 Subscriber Obligations

When requesting and using a certificate issued under this CPS, a subscriber accepts the following obligations:

- To ensure the accuracy of all information submitted to and contained in the certificate,
- To protect the certificate private key from unauthorized access in accordance with section 4.6.2,
- To immediately report to the RA and request certificate revocation if private key compromise is suspected,
- To use the certificate only for authorized applications which have met the requirements of this CPS, and
- To report any changes to information contained in the certificate to the appropriate RA for certificate reissue.

4.2.1.6 Relying Party Obligations

When accepting a certificate issued under this CPS, a relying party accepts the following obligations:

- To ensure that the certificate is being used for an appropriate approved purpose,
- To check for certificate revocation or suspension prior to accepting the certificate,
- To verify the digital signature of the CA who issued the certificate they are about to use,
- To establish trust in the CA who issued the certificate by verifying the chain of CA certificates starting from the NA PKI Root CA, and
- To acknowledge all warranty and liability limitations.

4.2.1.7 Repository Obligations

Each CA within the NA PKI shall post certificates and CRL information in an LDAP enabled directory. Only information contained in the certificate shall be posted in this directory to ensure compliance with the Privacy Act. Access shall be via an interoperable

implementation of the Lightweight Directory Access Protocol (LDAP). Access will also be available via Hypertext Transfer Protocol (HTTP) through a directory gateway interface.

The certificate repository shall meet the following obligations:

- To list all unexpired certificates for the respective CA to relying parties;
- To contain an accurate and current CRL for the respective CA for use by relying parties;
- To be publicly accessible through a web server gateway using HTTPS and FIPS 140-1 approved encryption;
- To be maintained in accordance with the practices specified in this CPS; and
- To meet or exceed the requirement of 99% availability for all components within the control of the operating organization. *[NOTE: Communication failures as a result of Internet problems external to the operating organization shall not count against this availability requirement.]*

4.2.1.8 Cross-Certified CA Obligations

Any CA from an external PKI wishing to cross-certify with the NA PKI at any level within the hierarchy shall meet or exceed all requirements listed in section 4.2.1. In addition, a CA that is cross-certified with any CA in the NA PKI accepts the following obligations:

- To notify the cross-certified CA of any CPS modifications; and
- To notify the cross-certified CA if any CA private key within the cross-certifying PKI is believed compromised.

4.2.2 Liability

4.2.2.1 Warranties and Limitations On Warranties

The NA PKI Certificate Authority Administrator (CAA) warrants that all procedures are implemented in accordance with this CPS, and that any issued certificates that assert the policy OID identified in Section 2.1.2 were issued in accordance with the stipulations of this policy.

4.2.2.2 Damages Covered and Disclaimers

Without limiting other subscriber obligations stated in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one

or more digital signatures with the certificate, reasonably rely on the representations contained therein.

The NA PKI CAA disclaims all warranties and obligations of any type other than those listed in Section 4.2.2.1.

4.2.2.3 Loss Limitations

The NA PKI CAA disclaims any liability for loss due to use of certificates issued by the NA PKI provided that the certificate was issued in accordance with this CPS. If any CA or IAs is negligent, reckless, or engages in fraudulent activity, the NA PKI CAA shall not be liable for more than $1 million (U.S. Dollars) total liability.

4.2.2.4 Other Exclusions

No stipulations.

4.2.3 Financial Responsibility

4.2.3.1 Indemnification By Relying Parties and Subscribers

Agents of the NA PKI assume no financial responsibility for improperly used certificates.

4.2.3.2 Fiduciary Relationships

Issuance of certificates in accordance with this CPS does not make any CA, IA, RA, or TA, an agent, fiduciary, trustee, or other representative of subscribers or relying parties. The relationship between the NA PKI and its designated agents and subscribers and that between the NA PKI and its designated agents and relying parties is not that of agent and principal. Neither subscribers nor relying parties have any authority to bind the NA PKI or its designated agents, by contract or otherwise, to any obligation. The NA PKI and its designated agents shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

4.2.3.3 Administrative Processes

No stipulation.

4.2.4 Interpretation and Enforcement

4.2.4.1 Governing Law

The laws of the United States of America shall govern the enforceability, construction, interpretation, and validity of this CPS.

Various laws and regulations may apply based on the jurisdiction in which a certificate is issued or used. It is the responsibility of the certificate holder or user to ensure that all applicable laws and regulations are adhered to.

4.2.4.2 Severability of Provisions, Survival, Merger, and Notice

No stipulation.

4.2.4.3 Dispute Resolution Procedures

An attempt shall be made to resolve any dispute through an independent mediator, mutually agreed to by all disputing parties.

If mediation is unsuccessful in resolving a dispute, it shall be resolved by arbitration in accordance with applicable statutes. *[NOTE: Procedures for dealing with the resolution of disputes that cross national borders are yet to be determined.]*

4.2.5 Fees

4.2.5.1 Certificate Issuance or Renewal Fees

No fee shall be levied by any CA or IA within the NA PKI to issue or renew a certificate to government employees or government-owned servers.

No fee shall be levied by any CA or IA within the NA PKI to issue or renew a certificate to a contractor employee requiring access to government resources, a contractor-owned server used in support of Navy contracts, a foreign national requiring access to government resources, or an organization requiring access to government resources.

Fees levied by cross-certified CAs to issue or renew certificates are at the discretion of the agency maintaining the CA.

4.2.5.2 Certificate Access Fees

No fee shall be levied for access to information about any certificate issued by any CA within the NA PKI.

Fees levied by cross-certified CAs to access certificate information are at the discretion of the agency maintaining the CA. Access fees are not recommended. Access fees shall be stated at the time of cross-certification and may affect ability to cross-certify.

4.2.5.3 Revocation or Status Information Access Fees

No fee shall be levied for access to revocation or status information about any certificate issued by any CA within the NA PKI.

Fees levied by cross-certified CAs to access revocation or status information are at the discretion of the agency maintaining the CA. Information access fees are not recommended. Information access fees shall be stated at the time of cross-certification and may affect ability to cross-certify.

4.2.5.4 Fees for Other Services Such as Policy Information

No fee shall be levied for on-line access to policy information about the NA PKI. A reasonable fee to cover media reproduction and distribution costs may be levied for a physical media copy of this policy information.

At least one copy, either on-line or physical media, of policy information about cross-certified CAs shall be made available to the cross-certifying CA at no charge at the time of cross-certification. At least one copy shall also be made available to the cross-certifying CA in the event of any changes to policy information.

Any fees levied by cross-certified CAs for other services, including additional copies of policy information, shall be stated at the time of cross-certification.

4.2.5.5 Refund Policy

No stipulation.

4.2.6 Publication and Repository

4.2.6.1 Publication of CA Information

Each CA within the NA PKI shall maintain a publicly accessible repository that shall contain, at a minimum:

- A listing of all current certificates signed by the CA;
- A current and accurate CRL;
- This CPS; and
- Any additional policy or practice information that is supplemental to this CPS.

4.2.6.2 Frequency of Publication

Certificates shall be accessible from the repository at the time of issuance. CRL publication shall be in accordance with section 4.4.4.3.1. The CPS shall be published in accordance with section 4.8.2.

4.2.6.3 Access Controls

There shall be no access controls on the reading of this CPS, any supplemental policy information, or any supplemental practice information published by the NA PKI. Certificate and CRL information shall be publicly available.

There shall be no access controls on the repository information, including certificates and CRLs. Repository updates shall be restricted to authorized individuals.

4.2.6.4 Repositories

Each CA shall maintain a repository containing the information identified in section 4.2.6.1. This repository may be maintained directly by the CA or by another authorized organization.

4.2.7 Compliance Audit

4.2.7.1 CA Audit

4.2.7.1.1 Frequency of Entity Compliance Audit

CA Compliance audits will be accomplished every six months.

4.2.7.1.2 Identity / Qualifications of Auditor

The CA Information Systems Security Officer (ISSO) in conjunction with any interested relying party Information Systems Security Manager (ISSM) will conduct the audit.

4.2.7.1.3 Auditor's Relationship to Audited Party

The CA ISSO is independent of the CAA and the SA. If the ISSM and the ISSO roles are performed by different individuals, the ISSO shall report to the ISSM.

4.2.7.1.4 Topics Covered by Audit

- Review the CA Access Log noting any suspicious recurring access by any single source.
- Review the CA Error Log ensuring that there is a minimum of errors attributable to understood and explainable phenomena.
- Review the CA Service Log and note that only authorized IAs are issuing certificates.
- Review the CA Analysis Report noting any suspicious client access profiles.
- Review that the archives both on-site and off are being maintained.

4.2.7.1.5 Actions Taken as a Result of Deficiency

Any discrepancies between a CA's operation and the stipulations of its CPS shall be noted. If the discrepancies are determined to increase financial risk, the underwriting agency will be made aware, and actions will be taken in accordance with the agreement between that agency and the PKI. If a discrepancy is determined to pose a security risk, the policy contacts shall be notified immediately. A remedy will be determined, including a time for completion. Any remedy may include permanent or temporary CA cessation, but several factors shall be considered in this decision, including the severity of the discrepancy and the risks it imposes, and the disruption to the certificate using community.

Remedies shall be defined and communicated to such a CA as soon as possible to limit the risks created. A parent CA may immediately terminate a CA's operation by revoking its certificate. This event should be a rare occurrence, precipitated by a catastrophic loss of trust in the CA. The implementation of remedies shall be communicated to the appropriate authority. A special audit may be required to confirm the implementation and effectiveness of the remedy.

4.2.7.1.6 Communication of Results

A written report by the ISSO documenting the audit results will be filed with the CAA of the Acquisition Root CA within one week of the audit. Any CA found not to be in compliance with its CPS or this policy shall be notified immediately at the completion of the audit.

4.2.7.2 IA Audit

4.2.7.2.1 Frequency of Entity Compliance Audit

IA compliance audits will be accomplished bi-monthly.

4.2.7.2.2 Identity / Qualifications of Auditor

The CA ISSO in conjunction with any interested relying party ISSO will conduct the audit.

4.2.7.2.3 Auditor's Relationship to Audited Party

The CA ISSO is independent of the CAA and SA. If the ISSM and the ISSO roles are performed by different individuals, the ISSO shall report to the ISSM.

4.2.7.2.4 Topics Covered by Audit

- Review the certificates issued by individual IAs for each CA during the reporting period and ensure a corresponding validation document from the cognizant RA.
- Review that the archives are being maintained

4.2.7.2.5 Actions Taken as a Result of Deficiency

Any discrepancies between an IA's operation and the RA's approval shall be noted. If the discrepancies are determined to be negligence, the underwriting agency will be made aware, and actions will be taken in accordance with the agreement between that agency and the PKI. If a discrepancy is determined to pose a security risk, the subject certificate shall be revoked and any commanding/employing authority shall be notified immediately.

Remedies shall be defined and communicated to such an IA as soon as possible to limit the risks created. The CAA may immediately terminate an IA's operation by revoking their certificate in the event of reported discrepancy. The implementation of remedies shall be communicated to the appropriate authority. A special audit may be required to confirm the implementation and effectiveness of the remedy.

4.2.7.2.6 Communication of Results

A written report by the ISSO documenting the audit results will be filed with the CAA within one week of the audit. Any CA found not to be in compliance with its CPS or this policy shall be notified immediately at the completion of the audit.

4.2.7.3 RA Audit

4.2.7.3.1 Frequency of Entity Compliance Audit

RA compliance audits will be accomplished periodically.

4.2.7.3.2 Identity / Qualifications of Auditor

The NA PKI command ISSO will conduct the audit.

4.2.7.3.3 Auditor's Relationship to Audited Party

The ISSO may have a direct working relationship with the RA.

4.2.7.3.4 Topics Covered by Audit

- Review that newly designated RAs have received training.
- Review that RA archives of validated certificates are being retained in physical (paper) and/or electronic (email) format.
- Review that RA validation and submission procedures are being followed.
- Review any associated TA audit records and ensure that any TAs are following the stipulations of this CPS.

4.2.7.3.5 Actions Taken as a Result of Deficiency

Ensure that proper training is conducted and documented. Ensure that a proper system is available for archiving validation records.

4.2.7.3.6 Communication of Results

A written report by the ISSO documenting the audit results will be filed with the CAA within one week of the audit. Any RA found not to be in compliance with its CPS or this policy shall be notified immediately at the completion of the audit.

4.2.7.4 TA Audit

4.2.7.4.1 Frequency of Entity Compliance Audit

TA compliance audits will be accomplished twice per year.

4.2.7.4.2 Identity / Qualifications of Auditor

The program RA will conduct the audit.

4.2.7.4.3 Auditor's Relationship to Audited Party

The RA will have a direct working relationship with the TA.

4.2.7.4.4 Topics Covered by Audit

- Review that newly designated TAs have received training and signed an acceptance of that training.
- Review that TA archives of validated certificates are being retained in physical (paper) and/or electronic (email) format.
- Review that TA validation and submission procedures are being followed.

4.2.7.4.5 Actions Taken as a Result of Deficiency

Ensure that proper training is conducted and documented. Ensure that a proper system is available for archiving validation records.

4.2.7.4.6 Communication of Results

The RA will file a written report documenting the audit results for review by the command ISSO at the RA audit. Any TA found not to be in compliance with its CPS or this policy shall be notified immediately at the completion of the audit.

4.2.7.5 Subscriber Audit

There are no audit requirements for the subscriber.

4.2.8 Confidentiality

4.2.8.1 Types of Information to be Withheld from Release

Information requested from individuals during the certificate issuance process other than that information, which is specifically included in the certificate, shall be withheld from release. This information may include personal information subject to the Privacy Act. All information in the CA record (not repository) shall be handled as SBU, and access shall be restricted to those with official needs.

Certificate private keys shall be considered sensitive and access shall be restricted to the certificate owner.

Private keys held by a CA shall be held in strictest confidence. Under no circumstances shall any private key appear unencrypted outside the CA hardware. Private keys held by a CA shall be released only to a trusted agency authority in accordance with this CPS, or

a law enforcement official, in accordance with US law and this policy (see section 4.2.8.4).

Although records of individual transactions may be released in response to reasonable information requests, audit logs as a whole are considered sensitive and shall not be made available.

4.2.8.2 Types of Information Not Considered Sensitive

Sensitive information shall not be held in certificates as certificate information is publicly available in repositories. This information includes the subscriber's name, electronic mail address, certificate public key, and certificate validity period.

4.2.8.3 Disclosure of Certificate Revocation / Suspension Information

The CRL for each CA shall be updated in accordance with section 4.4.4.9. This information shall be publicly available in the CA repository. Information concerning the revocation of a certificate or events leading to such a revocation should be limited to the individuals involved.

4.2.8.4 Release to Law Enforcement Officials

Sensitive data shall be released to law enforcement officials only under a proper court order as confirmed by local Navy command lawyers.

4.2.8.5 Release as Part of Civil Discovery

Sensitive information shall be released to civil authorities only under a proper subpoena as verified by local command lawyers

4.2.8.6 Disclosure Upon Owner's Request

No stipulation.

4.2.8.7 Other Information Release Circumstances

Release of information shall be handled under the existing procedures for data release in the Freedom of Information Act.

4.2.9 Intellectual Property Rights

Certificates are the property of the issuing CA.

Public and private keys are the property of the rightful key holder for individual certificates (CA, IA, RA, or subscriber), or the property of the designated responsible party for server subscriber certificates.

Unless otherwise agreed, property interests in the following security-related information materials and data are regarded as the property of the parties indicated below:

- Certificates are the personal property of their respective CA. Permission is granted to reproduce and distribute certificates issued by NA PKI CAs and Navy Acquisition subordinate CAs on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Certificates shall not be published in any publicly accessible repository or directory without the express written permission of NA PKI.
- This CPS is the personal property of NAVSUP, NAVAIR, and Operational Research Consultants.
- Private keys are the personal property of the subscribers who rightfully use or are capable of using them (or their employer or principal), regardless of the physical medium within which they are stored and protected.
- Public keys are the personal property of subscribers (or their employer or principal), regardless of the physical medium within which they are stored and protected.
- NA PKI CA public keys, including root CA public keys, are the property of NA PKI. NA PKI licenses relying parties to use such keys only in conjunction with FIPS 140-1 validated encryption modules.

4.3 IDENTIFICATION AND AUTHENTICATION

4.3.1 Initial Registration

This section contains the practices to be followed in identifying and authenticating individuals involved in the certification request process.

4.3.1.1 Types of Names

Certificate requests shall include a distinguished name including a Simple Mail Transport Protocol (SMTP) electronic mail address. Distinguished names consist of a combination of a common name and a Relative Distinguished Name (RDN). Common names are either full names for individuals or Uniform Resource Locators (URLs) or IP addresses for application servers. RDNs include identification information about the individual making the request, including the company for contractors and organizations or the country for foreign nationals, both fitting in an Organization Unit field.

4.3.1.2 Need for Names to be Meaningful

Common names shall be meaningful as individual names or as actual server URLs or IP addresses. Company names listed in RDNs shall be legitimate for use by the certificate requestor.

4.3.1.3 Rules for Interpreting Various Name Forms

No stipulation.

4.3.1.4 Uniqueness of Names

Distinguished names shall be unique. Common names do not need to be unique, but the combination of the common name and the RDN shall be unique. The use of electronic mail address as the login ID in the distinguished name insures uniqueness of names.

4.3.1.5 Name Claim Dispute Procedure

Issuing Authorities shall investigate and correct if necessary any name collisions brought to their attention.

4.3.1.6 Recognition, Authentication and Role of Trademarks

In general, use of trademarks in a name form or as any part of a name form is discouraged. Trademarks shall not be used as a name form or as a part of the name form for certificates issued to government employees unless they are held by the U.S. Government personnel or devices have a legitimate right to their use. Trademarks in certificates issued to contractors, contractor-owned servers, foreign nationals, or organizations shall only be used with specific permission by the holder of the trademark.

4.3.1.7 Method to Prove Possession of Private Key

Proof of Possession is accomplished through the use of the Netscape KEYGEN tag for certificate request to prove possession to the CA when submitting a certificate request, combined with a separate check by the browser itself when retrieving the certificate and installing it for use.

The CA supplies a random challenge string to the browser as part of the KEYGEN tag. The public key generated by the browser and the challenge string supplied by the CA are DER encoded together, and the resulting PublicKeyAndChallenge value is then digitally signed with the private key to produce a SignedPublicKeyAndChallenge value. This signed value is then base 64 encoded and sent to the CA as part of the certificate request;

the CA verifies the signature using the included public key, thus proving possession by the browser of the private key corresponding to that public key.

The public key and challenge strings are DER encoded as PublicKeyAndChallenge and then digitally signed with the private key to produce a SignedPublicKeyAndChallenge. The SignedPublicKeyAndChallenge is base64 encoded, and the ASCII data is finally submitted to the server as the value of a name-value pair, where the name is specified by the NAME attribute of the KEYGEN tag. When retrieving the completed certificate the browser also checks before importing the certificate into its database, to verify that the public key in the certificate being installed matches the private key it originally generated.

An additional out of band check is preformed by requiring the requestor to print the base 64 of the DER encoded certificate request and present it in person during the validation process. The RA validates both the person's identity and their possession of a certificate request corresponding to their private key.

4.3.1.8 Authentication of Organization Identity

Users shall provide proof of their employment by the government or relationship to the company they work for. This proof can be done by:

- Applicant providing a current government civilian or military ID,
- Applicant presenting a government-issued photo badge including the applicants company affiliation,
- Applicant requesting a certificate accompanied by a government sponsor who attests to the employment of the individual by the named company,
- Applicant including a signed letter from an authorized organization official attesting to the relationship, or
- Applicant presenting an unexpired photo badge issued by the organization.

4.3.1.9 Authentication of Individual Identity

4.3.1.9.1 CA Authentication

Authentication of CA certificates shall be performed only by the CAA. Each CA shall be accredited by the CAA of the parent CA to ensure compliance with the requirements of this CPS. The CAA shall record the process that was used to establish and authorize the CA.

4.3.1.9.2 IA Authentication

Authentication of at least one IA certificate shall be performed at the time of accreditation of the CA by an authorized agent of the parent CA. Authentication of additional IAs may be performed by IAs or by an authorized agent of the CA.

Government employee IAs shall present, in person, a picture identification, either a military or government identification card, and proof of a current favorably adjudicated personal security investigation. Contractors acting as authorized agents shall present, in person, a photo ID and proof of employment. The CA accreditation agent or IA granting the IA certificate shall record the identification and authentication process that was used to establish the IA's identity.

4.3.1.9.3 RA Authentication

IAs or RAs shall authenticate RAs. RAs shall present, in person, a picture identification, either a military or government identification card. If the RA is a government employee and is personally well known to the agent performing the authentication, RAs may be authenticated over the phone. Contractors acting as authorized agents shall present, in person, a photo ID and proof of employment. The agent performing the identification shall record the identification and authentication process that was used to establish the RA's identity.

4.3.1.9.4 TA Authentication

RAs shall authenticate TAs. TAs shall present, in person, a picture identification, either a military or government identification card to the RA. If the TA is a government employee and is personally well known to the RA performing the authentication, TAs may be authenticated over the phone. Contractors acting as authorized agents shall present, in person, a photo ID and proof of employment. The RA performing the identification shall record the identification and authentication process that was used to establish the TA's identity.

4.3.1.9.5 Subscriber Authentication

4.3.1.9.5.1 Government Employee

RAs or TAs shall authenticate government employees. Generally, the subscriber shall present, in person, a picture identification, either a military or government identification card. If the subscriber is personally well known by the RA, the RA shall verify that the request actually came from the named subscriber, but no additional identification or authentication is required. Applicants requesting authentication from a TA must present, in person, a picture identification.

4.3.1.9.5.2 Government-Owned Server

RAs shall authenticate government-owned servers. Servers shall not be authenticated unless they have been accredited or granted Interim Authority to Operate (IATO) by the local ISSM. Accreditation or IATO shall be granted according to the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The individual holding primary responsibility for the server shall verify that appropriate accreditation information is contained in the server certificate request. Authentication of this individual shall be performed in accordance with the appropriate subscriber authentication procedures.

4.3.1.9.5.3 Contractor Employee

RAs or TAs shall authenticate contractors. If the subscriber has a valid government identification card, the subscriber shall present, in person, that card. If the subscriber does not have a government issued identification card, the subscriber shall present, in person, a picture identification card and be accompanied by a government sponsor.

4.3.1.9.5.4 Contractor-Owned Server

RAs shall authenticate contractor-owned servers. Servers shall not be authenticated unless they have been accredited or granted IATO by the local ISSM. The individual holding primary responsibility for the server shall verify that appropriate accreditation information is contained in the server certificate request. A valid contract number or other indication of the requirement to process government information shall be required at the time of certificate verification. Authentication of the individual holding primary responsibility for the server shall be performed in accordance with the appropriate subscriber authentication procedures.

4.3.1.9.5.5 Foreign National

RAs shall authenticate foreign nationals. If the subscriber has a valid government identification card, the subscriber shall present, in person, that card. If the subscriber does not have a government issued identification card, and is physically colocated with an RA, he or she shall present, in person, proof of identity, proof of requirement to access a government resource, and be accompanied by a government sponsor. If the subscriber is not physically colocated with a RA, he or she shall present authorized paperwork in accordance with existing identification policies to the RA. *[NOTE: Foreign National certificate issuance processes are pending legal review at this time.]*

4.3.1.9.5.6 Organization

RAs shall validate authorized representatives of organizations seeking to do business with NA PKI protected applications. Organization representatives shall present an original signed letter requesting authentication to the organization RA. This letter shall state, at a

minimum, the name and address of the company, the name or names of individuals authorized to request individual certificates for that company, and a statement that the company accepts the policies outlined in this CPS. The letter shall be signed by a company official. The organization RA shall verify the company in accordance with existing identification policies for vendors seeking to do business with the government..

4.3.2 Routine Re-key

Because of the pilot status of the NA PKI, certificates issued by the NA PKI shall have a validity period of one year. If the NA PKI has not been migrated to the DoD PKI, subscribers may request new certificates without the need to revalidate identity prior to expiration of their current certificates. The subscriber will be required to present a currently valid certificate to request a new certificate. This process will be permitted twice, after which identity must be established as for a new request. It is anticipated that the NA PKI will be migrated to the DoD PKI prior to the expiration of this three year renewal period. End users may renew their certificates through a web based electronic form.

During the renewal process the user must present his or her current signature certificate during an SSL client authentication to the CA. The CA validates the authenticity of the certificate being presented by verifying that the certificate was issued by the CA in question and mapping the subject name in the certificate to its corresponding certificate in the database. The forms to accomplish the this process are controlled by access control lists on a secure web server that bind to corresponding users with certificates in an LDAP directory. Access control to the renewal forms is based on comparing the certificate with Distinguished Name of the subscriber (based on an X.509 certificate-based authentication) against the certificate with Distinguished Name in the directory.

4.3.3 Re-key After Revocation

Identification and authentication of individuals for rekey after certificate revocation requires following the steps outlined in section 4.3.1.9. If private key compromise is suspected, additional steps shall be taken to minimize key compromise risk as outlined in section 4.4.4.1.3.

4.3.4 Revocation Request

Certificate revocation requests may be made in using the same practices as certificate issuance requests in accordance with section 4.3.1.9. In addition, certificate revocation requests may be made electronically using digitally signed electronic mail. See section 4.4.4 for details on certificate revocation procedures.

4.4 OPERATIONAL REQUIREMENTS

4.4.1 Certificate Application

4.4.1.1 Submission of Request

Certificate requests shall be made by the individual requiring the certificate, or by the designated responsible party for servers. The request will be made from the primary workstation of the subscriber via a web interface.

When making the certificate request, the applicant shall submit a proposed distinguished name in accordance with local naming conventions, generate the public private key pair using FIPS 140-1 approved software, and submit information and the public key to the CA for issuance.

The applicant shall protect the private key with a password or pass phrase. This password shall be kept confidential and shall not be recorded or given to any other parties except in accordance with locally approved key escrow procedures. The same password may be used to protect multiple private keys for the same individual.

The applicant shall make the request using a web browser incorporating a FIPS 140-1 cryptographic module for generating the key pair and submitting the required information through an on-line form. *(Note: Currently only Netscape Navigator, version 4.08 or higher, meets this requirement.)*

4.4.1.2 Validation of Request

All certificate requests shall be validated through the authentication procedures in section 4.3.1.9. The applicant will be notified by the appropriate validation authority of the certificate request and be asked to present the required information. Notification shall be done out-of-band, by telephone or personal visit.

The validating authority shall either physically sign a printed form or digitally sign an electronic mail message indicating approval of the certificate request. This form or message shall be forwarded by the RA to the IA.

4.4.2 Certificate Issuance

The IA shall issue certificates upon receipt of both the certificate request and the verification package. The IA shall verify that the verification procedure has been correctly and completely followed before issuing a certificate to the applicant.

The IA shall verify the ink or electronic signature of the email from the RA and shall verify that the public key information contained in the email matches the information in the certificate request.

The IA shall notify the certificate applicant of certificate issuance through electronic mail. The notification shall include the URL that the applicant will use to receive the approved certificate. The IA shall also publish the certificate in the repository at the time of issuance.

4.4.3 Certificate Acceptance

After receiving the email notification from the IA, the applicant shall go to the URL specified in the message to accept the certificate. The CA shall verify possession of the public key at the time the applicant accepts the issued certificate in accordance with section 4.3.1.7.

Certificate shall be stored locally by the user to prevent private keys from being transmitted over a network. Certificates may be stored on workstation hard drives if they are encrypted and password protected with a password of at least 8 characters in length. Certificates may also be stored on floppy disks or on hardware tokens such as smart cards. If multiple certificates belonging to multiple individuals are stored on the same workstation, each individual must have their own password protected method for storing the certificate, (e.g. different profiles).

By accepting a certificate, the applicant acknowledges agreement to the terms and conditions contained in the CPS and in any local policies.

4.4.4 Certificate Suspension and Revocation

4.4.4.1 Revocation

Requests for certificate revocation shall either be digitally signed by the individual making the request, or the individual shall follow the same procedures outlined in section 4.3.1.9 to present the request to the RA.

4.4.4.1.1 Circumstances for Revocation

Certificates may be revoked in the following circumstances:

- The certificate holder requests that the certificate be revoked;
- The certificate holder can be shown by an RA, TA, or other trusted party to have violated the subscriber obligations, including payment of any required fees,

- The certificate holder is no longer authorized to hold the certificate (e.g. termination of employment or change in responsibilities);
- The information in the certificate is no longer accurate; or
- Certificate private key compromise is suspected.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Certificates shall remain on the CRL until they expire. They shall be removed after they expire, but must at least appear in one CRL.

4.4.4.1.2 Who Can Request a Revocation

Any subscribersubscriber may request revocation of their own certificate(s) and RAs may request revocation of any subscribersubscriber's certificate on behalf of the subscribersubscriber or other authorized party. IAs and CAs may revoke any certificate within its domain for reasons identified in this CPS.

If any individual has reason to believe that a certificate private key has been compromised, that individual is required to tell a RA or IA of the compromise suspicion. It is the responsibility of the RA or IA to investigate the information and determine if certificate revocation is warranted.

Other parties may also request revocation of certificates through any RA, for example as a part of the exit interview process. The RA shall validate the credentials of the requesting party, and shall determine if the revocation request meets the requirements of section 4.4.4.1.1. If so, the RA shall forward the revocation request along with documentation of the reason for the request to the IA.

4.4.4.1.3 Revocation Request Procedure

The RA reviews all revocation requests to ensure that the revocation requests are legitimate and will then inform the IA of the revocation request by signed electronic mail or signed fax. The IA will perform the revocation. A CRL entry will be created for the revoked certificate and will be added to the CRL list. An entry for a revoked certificate shall be retained on the CRL until that certificate's expiration date has passed. In addition, all revocations shall be maintained in an archive. The request to the RA will be by signed electronic mail, signed fax, or in person.

If the individual making the certificate revocation request is not the individual named in the certificate being revoked, the requester shall notify the certificate holder as soon as possible through a phone call or electronic mail message. If the certificate was revoked because of suspected key compromise, the entity responsible for verifying the certificate shall also be notified.

If the IA is choosing to revoke a certificate because of sufficient evidence of noncompliance with this CPS, the IA shall document the reason for certificate revocation and shall notify the subscriber of the revocation.

If the circumstances justify it, or if there is no outstanding reason to deny the request, the IA shall revoke the certificate by placing its serial number and other identifying information on a Certificate Revocation List (CRL). The IA shall also remove the certificate from the master directory and any replicated directories

4.4.4.1.4 Revocation Request Grace Period

Certificates shall be revoked upon request. There is no grace period.

4.4.4.2 Suspension

This CPS does not support certificate suspension.

4.4.4.3 Certificate Revocation Lists

4.4.4.3.1 CRL Issuance Frequency

The CRL shall be immediately updated whenever there is an addition to the list. The CRL will be immediately updated on the CA and the repository.

4.4.4.4 CRL Checking Requirements

It is the responsibility of the relying party to verify that certificates have not been revoked. Certificates may be stored locally by a relying party, but should be validated at least daily before use.

Any relying party that downloads the CRL shall verify the authenticity of the CRL by verifying the signature and associated certification path.

4.4.4.5 On-Line Revocation / Status Checking Availability

The CA shall make available to any relying party, via the repository and replicated directory servers, the ability to verify that any certificate issued by that CA has not been revoked.

The On-line Certificate Status-checking Protocol (OCSP) is not supported by the NA PKI at this time.

4.4.4.6 On-Line Revocation Checking Requirements

Relying parties shall validate certificates at least daily before use. This validation may be by verifying against a current CRL or through a replicated directory.

4.4.4.7 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.4.8 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.4.9 Special Requirements in Reference to Key Compromise

If a certificate is revoked because of suspicion of private key compromise, the following additional requirements apply in addition to requirements specified above.

- The CA shall notify, through web site posting, any relying parties that download the CRL that a certificate has been revoked because of key compromise, and the date that the suspected compromise occurred.
- The certificate holder shall notify known relying parties of the key compromise and the date the suspected compromise occurred.
- If the certificate was a RA certificate, the RA shall revalidate any subscriber certificates validated after the date of the suspected compromise, and shall revoke any certificates not revalidated.
- If the certificate was an IA certificate, the IA shall revalidate any certificates issued after the date of the suspected compromise and shall revoke any certificates not revalidated.
- If the certificate was a CA certificate, the CA, parent CA, System Administrator (SA), and Information Systems Security Manager shall determine the requirement for revoking the CA certificate and/or revoking and reissuing all or part of the certificates signed by the CA

4.4.5 Security Audit Procedures

NA PKI CA equipment shall record, for purposes of security audit, events as described below, whether the events are attributable to human action (in any role) or are automatically invoked by the equipment. At a minimum, the information recorded shall include the type of event, and the time the event occurred. In addition, for some types it will be appropriate to record the success or failure, the source of destination of a message,

or the disposition of a created object (e.g., a filename). Where possible, the audit data shall be automatically collected. When this is not possible a logbook or other physical mechanism shall be used. Logbook entries include: records of hardware and software maintenance, and designation of official personnel. Many RA responsibilities require out-of-band activity. Records of such activity shall be recorded in a logbook or other physical medium. A record of any paper forms or copies of photo IDs collected from users shall also be maintained.

4.4.5.1 Types of event recorded

NA PKI CAs shall record events related to the CA software and to CA processing. The events recorded may be attributable to human intervention or automatically invoked by the equipment. At a minimum, the information recorded shall include the type of event and the time the event occurred. Where appropriate, additional information may be recorded. Example information that may be collected follows.

Events related to the CA software

- Installation - name of installer, date of installation, and build information of any files installed.
- Software modification - name of modifier, date of modification, build information of any modified files, reason for modification.
- Configuration modification - changes in configuration files, security profiles, administrator privileges, and reason for modification.
- Logins and logouts - username and number and time of failed login attempts.

Events related to the CA processing:

- Certificate generation requests - sender DN, subject DN, and transaction ID.
- Certificate revocation requests - sender DN, issuer DN and serial number of certificate revoked, subject DN of certificate to revoke, revocation reason, transaction ID, and date of suspected compromise.
- CA responses - transaction ID, subject DN, and status of request.
- User confirmation - transaction ID, subject DN, and method of confirmation.
- CA actions - designation of IAs, execution of any IA duties, manual interactions with end entities, disclosure of information, access to IECA databases, and CRL generation.
- CA publications - certificate and CRL publication to directory, and changes to CPS.
- CA re-key - new certificate and list of designated IAs.
- Error conditions - receipt of improper messages.

4.4.5.2 Frequency of processing log

The logs will be processed and rolled once per month.

4.4.5.3 Retention period for audit log

Logs will be retained for a minimum of one year.

4.4.5.4 Protection of audit log

The audit log will not be open for modification by any human, or by any automated process other than those that perform audit processing. Archives shall be maintained on CD-ROM.

4.4.5.5 Audit log backup procedures

Audit logs will be backed up monthly to tape in conjunction with the review process.

4.4.5.6 Audit collection system (internal vs. external)

The audit system will be internal to the PKI equipment. NA PKI CAs shall invoke the audit processes at system startup and shall cease audit processes only at system shutdown.

4.4.5.7 Notification to event-causing subject

NA PKI CAs will not necessarily notify an entity of an auditable event caused by that entity.

4.4.5.8 Vulnerability assessments

System administrators and other operating personnel shall be watchful for attempts to violate the integrity of NA PKI CAs, including the equipment, physical location, and personnel.

4.4.6 Records Archival

4.4.6.1 Types of Data Archived

ORC will archive the audit log of all data identified in section 4.4.5.1.

4.4.6.2 Retention period for archive

Archived records shall be retained for seven years for all certificates, including CRLs and CA public keys. Each certificate shall remain in the archive for a period of seven years and six months past the expiration date.

4.4.6.3 Protection of archive

No user shall be able to write to, modify, or delete the archive. The archive shall be protected on-site in a safe certified for fire.

4.4.6.4 Archive backup procedures

The CA archives will be backed up monthly, labeled with the date and stored in a separate location under the control of individuals other than the designated Certificate Authority Administrator and the System Administrator.

4.4.6.5 Requirements for time-stamping of records

The backup and archiving of all records shall be time-stamped showing each time the data is backed up to tape. In addition, time-stamp information shall be kept in a physical paper log. Both electronic and paper forms of time-stamping shall indicate the date and time that each archive/backup process occurs, the data type, backup type, source of data, and any pertinent comments.

4.4.6.6 Archive collection system (internal or external)

Archive data shall be stored on Write Once Read Many (WORM) CDs. The archive data shall be collected at least on a monthly basis. Archive data is comprised of all log files and the certificate database. This information may be appended to a CD on a monthly basis. Twelve CDs will be used. When the archive data has been added to one CD, it will be moved to an off-site safe storage site and the oldest CD will be brought on-site for the next months archive data. The archive CD on-site will be kept at the same level of security as the computer from which it was copied or in the security approved safe.

4.4.6.7 Additionally, tape backups of the computer system will be accomplished. At least once a month the entire computer system will be backed up. Since this is a complete backup, the tape will also have the archive information on them. These complete backup tapes will also be kept offsite and will only be brought on-site when needed. Procedures to obtain and verify archive information

Archive data shall be restored from tapes using backup software to locate the desired data and restore it to the CA server. The CA ISSO shall verify that the appropriate directories

and files have been stored on tape by viewing the software record of the backup each month before the tape is taken off-site. The CA ISSO or other designated individual shall be responsible for removing the archive information to the off-site storage facility.

When archive information is needed, the CA ISSO shall be contacted to retrieve the data from the off-site storage. This person will then view the contents of the tape (using the backup software) to insure that the correct data is being retrieved.

4.4.7 Key Changeover

The NA PKI CAs will not issue certificates that extend beyond the expiration date of their own certificates and public keys. The NA PKI CA keys are valid for five years. It is not anticipated that renewal under the existing NA PKI structure will be required. If required, a new key will be generated at least one year prior to the expiration of the current certificate. The older, but still valid, certificate will be used to verify old signatures until all the user certificates signed under it have also expired.

4.4.8 Compromise and Disaster Recovery

4.4.8.1 Compromise

The procedures followed for compromise of a RA or IA private key are similar to compromise of a subscriber private key and are outlined in section 4.4.4.6.

Compromise of a CA private key is far more serious, since it may be possible for a holder of the compromised CA private key to create new certificates with “old” dates, it is impossible to verify that any certificate issued by that CA or by any child CA is valid. All keys under the hierarchy of the compromised key shall be revoked and reissued.

4.4.8.2 Disaster Recovery

The NA PKI CA contingency plan will come into effect only if an outage of more than 48 hours is anticipated. CA servers are not critical to daily PKI operation—instead, they are required only to create certificates for new users, to renew certificates, and to revoke certificates. Since the NA PKI CA servers will operate with back-up power and telecommunications, long outages are unlikely.

In the event of an extended outage, a second suite of equipment will be stood up as a temporary CA server. Backup tapes from the primary CA server will be used to synchronize the temporary CA server.

The NA PKI directory will be operated in a replicated configuration—that is two or more platforms located at different sites will contain replicas of the directory information. In the event one fails, users will still be able to obtain necessary information from the second directory server through Domain Name System (DNS) rotation schemes.

4.4.9 CA Termination

In the case of CA termination, all certificates issued under that CA will be revoked and the CA private keys will be destroyed so that they can not be compromised or otherwise used. Relying parties will be notified of the CA termination in a manner to ensure maximum dissemination of the revocation notice. Archive records for the terminated CA will be retained for seven years.

4.5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

4.5.1 Physical Controls

4.5.1.1 Site Location and Construction

The CA hardware physical location shall meet the following requirements:

- The site shall be located either within the continental U.S. or at a site controlled by a U.S. federal agency (e.g. on a U.S. military base);
- The site shall not be located in an area likely to flood (100 year flood plain), in an area likely to have an earthquake over a 6.0 on the Richter Scale, or any area likely to be destroyed or heavily damaged in a natural disaster that can occur on a periodic (50 year) basis;
- The building shall be owned by a U.S. company or the U.S. Federal Government;
- The building shall be constructed to require identification of individuals for entry;
- The suite shall be owned or leased by a U.S. federal agency or a U.S. company;
- If the CA is located at a commercial location, then the company shall have a contractual relationship with the U.S. Government for delivering CA services;
- The building shall be constructed to limit access to only individuals who shall identify themselves for entry;
- The room where the server is located shall be constructed to physically restrict access to unauthorized individuals; and

- The room where the server is located shall meet all construction and fire regulations required for computer rooms processing SBU data.

4.5.1.2 Physical Access

4.5.1.2.1 CA Physical Security Controls

Physical access to CA hardware, including the CA server, the firewall server, and any external cryptographic hardware tokens, shall be limited to those personnel performing one of the roles identified in section 4.5.2 or their authorized agents. Access to any media containing CA information shall also be physically protected and access shall be restricted to authorized personnel. CA information includes:

- Certificate database and database backups;
- CA private key and private key backups;
- The master CRL;
- Audit logs; and
- Archives.

[NOTE: Access restrictions do not necessarily apply to copies of audit log information or archive information made in response to authorized requests.]

A security check to the facility housing the CA's workstation shall be made at least once every 24 hours. If it is a continuously attended facility, this may be a visual check once per shift to ensure that the workstation and any associated cryptographic devices/tokens are securely stored if not in use, that the physical security systems (e.g., door locks and alarms) are functioning properly, and that there have been no attempts at forceful entry or unauthorized access. If the facility is not continuously attended, a security check shall be conducted and logged prior to the departure of the last person. Backup material and documentation shall be audited separately if not colocated in the CA facility.

Access to computer facilities shall be restricted to authorized personnel only. All unknown or unidentified persons shall be accompanied or challenged by personnel to prevent unauthorized access to IT resources and/or disclosure of sensitive data. Only authorized users shall have access to IT resources. Uncleared maintenance and cleaning personnel shall be escorted at all times while in central computer rooms and facilities. Maintenance personnel servicing CA resources shall have a favorably adjudicated personal security investigation. If clearance of maintenance and cleaning personnel is not possible, a waiver is required from the CA ISSM.

4.5.1.2.2 IA Physical Security Controls

IAs shall use a reasonably sturdy safe or lockable file cabinet to store records of subscriber registration requests, RA validation information, and IA private key or password information. The hardware workstation and software may be kept in a regular office environment.

If an IA's workstation holds sensitive subscribersubscriber information (including subscribersubscriber key materials), then the IA's physical security controls shall be equivalent to those of a CA as described in section 4.5.1.2.1.

IA workstations shall not be left unattended when the IA private key is in an unlocked state (i.e., when the Personal Identification Number (PIN) or password has been entered). Access to a workstation that contains an encrypted IA private key shall be secured or protected with an appropriate access control product.

4.5.1.2.3 RA Physical Security Controls

RAs shall use a reasonably sturdy safe or lockable file cabinet to store records of subscriber validation requests, validation information, and RA private key or password information. The hardware workstation and software may be kept in a regular office environment.

RA workstations shall not be left unattended when the RA private key is in an unlocked state (i.e., when the PIN or password has been entered). Access to a workstation that contains an encrypted RA private key shall be secured or protected with an appropriate access control product.

4.5.1.2.4 Subscriber Physical Security Controls

Subscribers shall physically protect any password or PIN that allows unlocking the certificate private key. Preferably, PINs and passwords should be memorized and not written down. If a PIN or password needs to be written down, it shall be stored in a locked file cabinet or container accessible only to authorized personnel.

If the subscriber uses a cryptographic token on which a private key is stored, the token shall be protected to an extent comparable with that of valuable personal items such as credit cards or a driver's license. The PIN or password used to unlock the token shall never be stored in the same location as the token itself. If a private key is stored encrypted on a diskette or other unsecured medium, such diskette or other medium shall be stored in a locked file cabinet or container when not in use.

Subscriber workstations shall not be left unattended when the private key is in an unlocked state (i.e., when the PIN or password has been entered). Access to a

workstation that contains an encrypted subscriber private key shall be secured or protected with an appropriate access control product.

4.5.1.3 Power and Air Conditioning

The CA facility shall have adequate power and backup power resources to provide CA uptime to the Internet with no more than a 48-hour downtime in any disaster period. All CA equipment and related hardware shall have sufficient backup power to have one hour of runtime after a power failure to provide for a normal shutdown.

A separate air conditioning unit shall be used as required to maintain the CA's operating environment within normal operating temperatures (70 degrees Fahrenheit +/- 5) for the equipment and personnel operating and administering the CA. At no time shall the lack of air conditioning be able to damage the CA equipment and cryptographic tokens.

IAs, RAs, and subscribers have no specific protection requirements for power and air conditioning.

4.5.1.4 Water Exposures

The CA's facility shall meet location requirements for flooding defined in section 4.5.1.1. The CA's room shall be located above ground and off of the floor by two feet to prevent internal flooding from damaging the CA equipment. All backup materials and CA documentation storage devices shall be constructed to prevent water damage or shall be located in areas not prone to water damage.

IAs, RAs, and subscribers shall protect any software or hardware tokens from water damage.

4.5.1.5 Fire Prevention and Protection

The CA building shall comply with all applicable national, state, and local fire regulations for a commercial office building. Fire prevention devices shall be enabled to eliminate or reduce fire and smoke damage to the CA equipment. Backup materials and documentation shall be located in fire resistant storage devices to reduce or eliminate damage to such materials.

IAs, RAs, and subscribers shall protect any software or hardware tokens from fire damage.

4.5.1.6 Media Storage

Removable media with CA, IA, or RA sensitive information shall be stored with appropriate physical protection as stated for other pieces of equipment. All removable media containing sensitive information shall be individually audited and accounted.

Magnetic media shall be stored in locations protected from accidental or intentional unauthorized erasures.

4.5.1.7 Waste Disposal

All sensitive CA, IA, and RA information shall be destroyed to prevent recovery of data and information according to the following guidelines:

- Paper or other records shall be shredded, disassembled, burned, or otherwise destroyed;
- Sensitive media shall be degaussed, disassembled, reformatted, burned, or otherwise destroyed to prevent recovery of data and information;
- CAs, IAs and RAs shall erase and reformat magnetic media that contain private key information; and
- Subscribers shall erase software-based tokens by simply deleting and overwriting the area on the disk containing.

If media containing licensed software is to be disposed of, software licenses shall be reviewed to ensure that the method of disposition and excess does not violate any licensing agreements.

4.5.1.8 Off-Site Backup

Backup media for critical data and programs shall be stored at a site sufficiently remote from the facility to preclude loss in the event of a disaster. The site where backup media is stored shall be subject to all requirements in section 4.5.1.1 except that the site may have a relationship with the contractor operating the CA site instead of directly with the U.S. Government.

4.5.2 Procedural Controls

4.5.2.1 Trusted Roles

4.5.2.1.1 CA Trusted Roles

To ensure that one person acting alone cannot circumvent safeguards, CA responsibilities shall be shared between multiple roles and individuals. Access permissions on the CA server shall be limited to capabilities required by the role.

There are four trusted roles relating to operation of a CA, the Certificate Authority Administrator (CAA), the System Administrator, the Information Systems Security Officer, and the CA Information Systems Security Manager.

The ISSO and ISSM perform oversight functions and are not directly involved in issuing certificates. The ISSO examines system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy. The ISSM examines records or audit logs of cross-certified systems to ensure that other CAs are acting within the realms of their responsibilities and within the agreed upon security policy.

CAA responsibilities include:

- Generation of CA certificates;
- Approval of IA certificates;
- Programming and secure distribution of subscriber hardware cryptographic tokens (if any);
- Generation, distribution, and management of CRLs;
- Administrative functions associated with maintaining the CA database; and
- Assisting in compromise investigations.

SA responsibilities include:

- Initial configuration of the CA server system including secure boot start-up and shut down of the workstation;
- Initial setup of all new accounts;
- Initial network configuration setup;
- Creation of emergency system restart media to recover from catastrophic system loss;
- Performing system backups;

- Software upgrades;
- System recovery from backup media; and
- Performing any required changes to the host name network address.

ISSO responsibilities include:

- Assigning security privileges and access controls of users;
- Assigning passwords to all new accounts;
- Performing archive of required system records;
- Reviewing and deleting the audit log to detect CAA compliance with system security policy.

ISSM responsibilities include:

- Review and approval of any cross-certification (within the administrative domain or between administrative domains); and
- Personally conducting or supervising an annual inventory of any cross-certified CA's records.

4.5.2.1.2 Other Trusted Roles

IAs, RAs, and TAs shall have designated command ISSOs who are responsible for audits including oversight in examining system records or audit logs to ensure that they are acting within the realms of their responsibilities and within the stated security policy.

IA, RA, and TA responsibilities are listed in sections 4.2.1.2, 4.2.1.3, and 4.2.1.4.

Command ISSO responsibilities include:

- Periodically review the certificates issued by the IA or validated by the RA for irregularities and non-compliance with procedures.

4.5.2.2 Number of Persons Required Per Task

For CA tasks, at least three distinct individuals shall perform the roles. The CAA and SA roles shall be performed by distinct individuals. The ISSO and ISSM roles may be performed by a single individual or by two distinct individuals. The ISSO and ISSM roles shall not be combined with CAA or SA roles.

CA key-pair generation and initialization of CA tokens shall require the active participation of at least a CAA and an ISSO. Startup of the CA system shall require the active participation of a CAA and a SA. Cross-certification of another CA shall require

the active participation of the CAA, ISSO, and ISSM with appropriate authorization documentation.

For IA, RA, or TA tasks, the ISSO shall be a distinct individual from the IA, RA, or TA.

4.5.2.3 Identification and Authentication for Each Role

All persons fulfilling one of the roles defined in section 4.5.2.1 shall be capable of identifying themselves to others with two forms of picture identification. One form shall be an official U.S. Government DoD identification or civilian contractor identification. Authentication may be established by calling or by signed electronic mail message from the verifying ISSO with CA oversight.

4.5.3 Personnel Controls

4.5.3.1 Background, Qualifications, Experience, and Clearance Requirements

4.5.3.1.1 CAA and SA

CAAs and SAs shall:

- Be of unquestionable loyalty, trustworthiness, and integrity;
- Have demonstrated security consciousness and awareness in all daily activities;
- Have a strong background in information technology resource administration and technical administration in either computer operations, system software, and/or application software totaling 12 months;
- Not be assigned other duties that would interfere with their CAA or SA duties and responsibilities;
- Not knowingly have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- Be a U.S. citizens;
- Have valid personal security investigations favorably adjudicated and be assigned to sensitive positions;
- Be appointed in writing by the ISSM; and
- Have received proper training in the performance of CAA or SA duties.

4.5.3.1.2 ISSO and ISSM

ISSOs and ISSMs shall:

- Be of unquestionable loyalty, trustworthiness, and integrity;
- Have demonstrated security consciousness and awareness in all daily activities;
- Have a technical understanding of the CA system they are providing oversight for;
- Not knowingly have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- Be a U.S. citizen;
- Have valid personal security investigations favorably adjudicated and be assigned to sensitive positions; and
- Have received proper training in the performance of ISSO or ISSM duties.

4.5.3.1.3 IA

IAs shall:

- Be of unquestionable loyalty, trustworthiness, and integrity;
- Have demonstrated security consciousness and awareness in all daily activities;
- Have a technical understanding of the CA system and the responsibilities of the IA within that system;
- Not knowingly have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- Be U.S. citizens;
- Have valid personal security investigations favorably adjudicated and be assigned to sensitive positions;
- Be appointed in writing by the ISSO; and
- Have received proper training in the performance of IA duties.

4.5.3.1.4 RA

The RA shall be trained in the verification policies and practices of this CPS and shall be trained in the performance of RA duties.

4.5.3.1.5 TA

The TA shall be trained in the verification policies and practices of this CPS and shall be trained in the performance of TA duties.

4.5.3.1.6 Command ISSO

Command ISSOs shall:

- Be of unquestionable loyalty, trustworthiness, and integrity;
- Have demonstrated security consciousness and awareness in all daily activities;
- Have a technical understanding of the CA system and of IA, RA, and TA responsibilities;
- Not knowingly have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- Be U.S. citizens;
- Have valid personal security investigations favorably adjudicated and be assigned to sensitive positions; and
- Have received proper training in the performance of ISSO duties.

4.5.3.2 Background Check Procedures

All personnel performing trusted roles, except RAs and TAs, shall be required to have a personal security investigation that has been favorably adjudicated and be assigned to sensitive positions.

The ISSO shall ensure that CAAs, SAs, ISSOs, and IAs meet the minimum qualifications before appointing the individual(s) to the positions.

Any maintenance or cleaning personnel that have physical access to CA servers or other sensitive information without an escort shall be subject to the same personal security investigation requirements as CAs and SAs.

4.5.3.3 Training Requirements

4.5.3.3.1 General Requirements

All personnel, who are military, civil servants, and contractors located or working on-site or accessing U.S. Government IT resources, shall receive INFOSEC awareness training annually. Additionally, periodic refresher training shall be provided to all personnel. The training program shall cover the requirements of the Computer Security Act of 1987, Public Law 100-235, which are adequately detailed in the Office of Personnel Management (OPM) Computer Security Awareness Training materials. The ISSM at each activity is responsible for managing this training.

4.5.3.3.2 CA Trusted Roles

Individuals responsible for CA trusted roles including CAAs, SAs, ISSOs, and ISSMs shall receive formal training. A formally trained CA ISSM may train other individuals with trusted roles for that CA. The parent CA ISSM is responsible for training the CA ISSM. The following training is recommended for all individuals with CA trusted roles:

- Training relative to the Privacy Act of 1974, information security, physical security, personnel security, and operations security; and
- Training relative to the activity's particular information technology resources, including operating systems analysis, hardware architecture, computer performance evaluation, and network concepts and operations.

Training in the following areas is required for CAAs:

- Course on administering a Certification Authority.

Training in the following areas is required for SAs:

- UNIX security course for the appropriate CA platform, and
- Firewall administration course on the proper operations of the dedicated firewall protecting the CA.

Training in the following areas is required for Command ISSOs:

- Appropriate course material to maintain ISSO qualifications.

4.5.3.3.3 Other Trusted Roles

The ISSO is responsible for providing training for other trusted roles within the CA. Actual training may be delegated to individuals who have been trained including IAs and RAs.

Training in the following areas is required for IAs:

- Security awareness and proper protection for cryptographic devices; and
- Course on IA responsibilities.

Training in the following areas is required for RAs:

- Security awareness and proper protection for cryptographic devices; and
- Course on RA responsibilities.

Training in the following areas is required for TAs:

- Course on TA responsibilities.

Training in the following areas is required for Command ISSOs:

· Appropriate course material to maintain ISSO qualifications.

4.5.3.4 Retraining Frequency and Requirements

No stipulation.

4.5.3.5 Job Rotation Frequency and Sequence

No stipulation.

4.5.3.6 Sanctions for Unauthorized Actions

4.5.3.6.1 Sanctions for CA Unauthorized Actions

Any unauthorized actions resulting in irreparable damage to a CA such as compromising the CA private key shall be treated very harshly. The responsible individuals may be prosecuted to the maximum of extent that the law affords, both criminal and civil.

4.5.3.6.2 Sanctions for IA Unauthorized Actions

Any unauthorized actions by an IA shall result in the immediate revocation of the IA certificate and the removal of that individual from the IA role. Certificates issued by that IA may also be revoked. The IA may be prosecuted for any damages caused to the Navy Acquisition PKI.

4.5.3.6.3 Sanctions for RA Unauthorized Actions

Any unauthorized actions by a RA shall result in the immediate revocation of the RA certificate and the removal of that individual from the RA role. Certificates validated by that RA may also be revoked. The RA may be prosecuted for any damages caused to the Navy Acquisition PKI.

4.5.3.6.4 Sanctions for TA Unauthorized Actions

Any unauthorized actions by a TA shall result in the immediate removal of that individual from the TA role. Certificates validated by that TA may also be revoked. The TA may be prosecuted for any damages caused to the Navy Acquisition PKI.

4.5.3.6.5 Sanctions for Subscriber Unauthorized Actions

Any unauthorized actions by a subscriber shall result in the immediate revocation of the subscriber certificate. The subscriber may be prosecuted for any damages caused to the Navy Acquisition PKI.

4.5.3.7 Contracting Personnel Requirements

Any company subcontracting to provide services for any trusted role with regards to this IECA shall require all employees delivering such services to be in accordance with this CPS and the policy identified in Section 4.1.2 and Section 4.5.3.

4.5.3.8 Documentation supplied to personnel

4.5.3.8.1 Certification Authority documentation

Operations and maintenance documentation shall be supplied to authorized individuals performing the roles of CAA and SA. An operations manual for CAs and an operations manual for SAs shall be written and managed for each logical instance of a CA and physical instance of a CA system.

The ISSM is responsible for maintaining the library for documentation and auditing its presence and content.

4.5.3.8.2 Other documentation

All other documentation including training material, standard operating procedures, cross-certification requirements, and help material will be made available to personnel through the web at *https://pki.navy.mil.*

4.6 TECHNICAL SECURITY CONTROLS

4.6.1 Key Pair Generation and Installation

4.6.1.1 Key pair generation

Key generation is used to generate a pair of keys (one private, the other public) that will be used for public key cryptographic functions (including symmetric key distribution and digital signature). The NA PKI will support both RSA-based and Digital Signature Standard (DSS) based functions. Both key exchange and digital signature RSA functions will be supported. DSS provides only the digital signature capability.

For the basic assurance PKI, users will generate the key pair locally. This may be done in a FIPS 140-1 Approved Web browser (such as Netscape Communicator).

4.6.1.2 Private key delivery to entity

If the key is generated by a user via a software process, and the key will be stored by and used by the application which generated it, no further action is required. Otherwise, the key shall be extracted for use by other applications or in other locations. Use of a protected data structure (such as defined in [PKCS#12]) is required. The resulting file may be kept on a magnetic medium, or transported electronically.

4.6.1.3 Public key delivery to certificate issuer

Public keys are delivered to the certificate issuer in a PKCS#10 certificate request.

4.6.1.4 CA public key delivery to users

The CA public key delivery to users allows users to trust the PKI created by the Navy Acquisition Root CA. Delivery of the Root CA public key which signifies trust of certificates issued by the CA is accomplished by accessing http://pki.navy.mil with the browser referenced in section 4.6.1.1 and pressing the "Accept the Navy Acquisition Authority Root" button to trust the PKI.

4.6.1.5 Key sizes

Key sizes for subscriber certificates shall be 1024 bits.

4.6.1.6 Public key parameters generation

Public key parameters for DSS shall be generated in accordance with FIPS 186.

4.6.1.7 Parameter quality checking

Parameters for Digital Signature Algorithm (DSA) shall be generated as specified in FIPS186.

4.6.1.8 Hardware/software key generation

IA keys shall be generated on cryptographic smart cards. IAs shall use smart cards from a vendor who has committed to FIPS 140-1 Level 2 certification and shall update cards and keys when certification has been obtained. End entities may use software or hardware tokens for key generation.

Random numbers for key material are to be generated by a FIPS 140-1 approved method.

4.6.1.9 Key usage purposes (as per X.509 v3 key usage field)

The use of a specific key is determined by the key usage extension in the X.509 certificate. This extension, its setting, and its processing, are described in section 4.7.1.2 of this policy. The key usage extension is currently not supported by the NA PKI but may be in the future as requirements dictate.

4.6.2 Private Key Protection

4.6.2.1 Standards for cryptographic module

All cryptographic modules shall have FIPS 140-1 key management capability; specifically, cryptographic keys may never be output in plain text. IAs and CAs shall use cryptographic modules that meet the criteria specified for Level 2 for all certificate management activities. IAs shall use hardware modules that are pending FIPS 140-1 Level 2 validation because there are no smart card tokens currently available that have been FIPS 140-1 Level 2 certified.

The CA keys are being migrated to Level 2 hardware tokens as the software is being migrated to Netscape CMS-4.1.

User	CA & IA
Level 1 with Level 2 key management	Level 2 with Level 3 key management

4.6.2.2 Private key (n out of m) multi-person control

None.

4.6.2.3 Private key escrow

Under no circumstances shall a signature key be escrowed.

For some purposes (such as data recovery), it will be necessary to escrow confidentiality keys. This feature will be implemented in accordance with the maturation of technology and law.

4.6.2.4 Private key backup

Users are requested to make backup copies of software based private keys when they accept their certificates. Backup copies shall be stored in an encrypted form and shall be protected by a password from unauthorized access. It is not recommended that software backups be made of hardware generated keys.

CA private keys may be backed up on a separate cryptographic module in order to obviate the need to rekey in the case of cryptographic module failure. When available, the backup module will be a hardware module that meets FIPS 140-1 level 2 requirements in general and level 3 key management requirements and will be under the protection of the CA administrator under lock and key at all times. When CAs are rekeyed, the private key in the backup module will be zeroized or destroyed.

4.6.2.5 Private key archival

Under no circumstances will a non-repudiation signature key be archived. Archival of confidentiality keys will be recommended if any information encrypted with those keys is archived in it's encrypted state.

4.6.2.6 Private key entry into cryptographic module

Private keys are to be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, a protected data structure (such as defined in PKCS#12) shall be used.

4.6.2.7 Method of activating private key

Subscriber private key is activated by password known only to the subscriber.

4.6.2.8 Method of deactivating private key

Cryptographic modules that have been activated shall not be left unattended or otherwise active to unauthorized access. Private keys stored in hardware tokens, including end user smart cards and CA hardware tokens, shall be removed from the token reader when not in use. CA hardware tokens shall be stored in accordance with section 4.5.1.2 when not in use.

Cryptographic modules that have been activated shall not be left unattended or otherwise open to unauthorized access. The subscriber shall set the browser to require the private key password after 15 minutes of inactivity.

4.6.2.9 Method of destroying private key

Private keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. The destruction method shall be in accordance with FIPS 140-1 requirements.

4.6.3 Other Aspects of Key Pair Management

4.6.3.1 Public key archival

The public key is archived as part of the certificate archival process in section 4.4.6.

4.6.3.2 Usage periods for the public and private keys

The key usage periods for keying material is described in section 4.3.2.

4.6.4 Activation Data

4.6.4.1 Activation data generation and installation

CAs, IAs, RAs, and subscribers shall use passwords to protect access to private keys. The passwords need not be automatically generated.

The password shall be in compliance with FIPS 112 or the DOD rainbow series password management guideline or best commercial practices. The minimum size for the password shall be at least eight characters with at least one alpha and one numeric character. Passwords shall be reset every three months. Currently, this password reset is a procedural requirement since currently available software does not allow for technically enforced password expiration, ORC shall require users to reset passwords every 3 months. The activation data (password) shall be generated by the user.

4.6.4.2 Activation data protection

Activation data should be memorized, not written down. If written down, it should be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

The cryptographic module shall protect the activation data as other critical security parameters in accordance with FIPS 140-1 requirements. Once FIPS 140-1 requirements are met, there are no additional requirements on the cryptographic module to further protect the activation data.

CA signing key passwords, use to unlock the hardware tokens, shall be protected by the CAA. The password will be written down and secured offsite, at a separate facility, stored in a General Services Administration approved security container (Mosler Safe).

The users shall protect their activation data from access by others. If the activation data is not entered directly in the cryptographic module, protocol shall be used so that the activation data is protected against eavesdropping and replay. Activation data shall never be shared.

4.6.4.3 Other aspects of activation data

No stipulation.

4.6.5 Computer Security Controls

Access to the CA server and related hardware shall be granted to trusted individuals only. The CA environment is part of a secure (locked) limited access computer lab. The CA server and related equipment shall be locked in an enclosed environment within the lab area accessible to a required limited sub-set of those who access the lab.

4.6.5.1 Specific Computer Security Technical Requirements

NA PKI CA equipment shall use a self-protecting operating system, that is, one that prevents and detects attempts to alter or to disable its security functions. An audit shall be carried out as described in Section 4.4.5. The operating system shall perform identification and authentication for individuals and actively enforce discretionary access controls on system and NACA application software and data. CA equipment shall additionally have design assurance for the operating system.

Security management control will include the execution of tools and procedures to ensure that the operational system and network adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

4.6.5.2 Computer Security Rating

NA PKI CA equipment shall meet and be operated at U.K. Information Technology Security Evaluation and Certification E2/F-C2 rating. This equates with C2 in the U.S. TCSEC / Orange Book. CA equipment shall operate at C2, and implement discretionary access control, object reuse controls, individual identification and authentication, and a protected audit record.

CA and network equipment uses the Solaris Basic Security Module (BSM) which provides the security features required by the C2 class of the Trusted Computer System Evaluation Criteria (TCSEC), that are not included in the standard Solaris 2.6 release. The additional features are the security auditing subsystem and a device allocation mechanism that provides the required object reuse characteristics for removable or assignable devices. C2 discretionary access control and identification and authentication features are provided by the standard Solaris system.

4.6.6 Life Cycle Technical Controls

Security management control will include the execution of tools and procedures to ensure that the operational system and network adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

- **Physical Safeguards:** The physical security safeguards and access controls shall continuously provide for protection against access or modifications to hardware/software by unauthorized individuals. In addition to the physical safeguards detailed in section 2.5.1, hardware tokens will be stored in a security container. CA and firewall CPUs, RAID/external drives, monitors, keyboards, and mice will be sealed with Tamper Resistant Seals in accordance with paragraph 8-308, ISM and Tab B, Code A, QUIC; in order to detect surreptitious entry into the equipment and associated peripherals. The seal will be inspected (and results logged) every month to ensure that it serves its intended use.

- **Access Controls:** Unescorted entry to the facility or access to any of its system components (hardware/software) shall be limited to personnel who are cleared for access and whose need to access has been confirmed by the CAA.

- **Equipment:** CA equipment is SUN hardware running the SOLARIS operating system connected to an external RAID disk system from Inline. The server is dedicated to administrating the key management infrastructure, has only CA software installed and is behind a firewall provided by Checkpoint (Firewall 1 V4), also on SUN hardware, that permits only https (in and out) and ldaps (out) to and from the network. All upgrades will be from the original equipment manufacturers and software vendors.

- **Upgrades:** Hardware and Software upgrades will be accomplished by the CA Administrator and SA in accordance with the Procedural Controls in section 4.5.2.

4.6.6.1 Development Environment Security

Assembly and maintenance of PKI systems will be accomplished in the controlled environment of the Server Room as described in section 4.5.1.1. Only personnel designated in the CPS will perform maintenance on the PKI systems. Hardware and Software upgrades will be accomplished by the CAA and SA in accordance with the Procedural Controls in section 4.5.2.

4.6.6.2 Configuration Management Security

PKI systems configuration management records are maintained by the ISSO as described in section 4.5.2.1. These records are stored in a locked container under the Security Auditor's control. Configuration management documents include CA signing key ceremony document, CA electronic forms, CA creation log, and procedures.

4.6.7 Network Security Controls

Access to the CA server and its data shall be protected by a firewall specifically allocated to protection of CAs. Only required accounts are present on the firewall. Hypertext Transfer Protocol over Secure Sockets Layer shall be the only type of data access that is allowed in. HTTP over SSL and Lightweight Directory Access Protocol are the only packet types allowed out. The firewall itself shall be secured in the locked CA environment area and not accessible over the network. All changes shall be made at the firewall station itself by an approved trusted individual.

Boundary controllers shall meet or exceed the requirements of the US Firewall Protection Profile. All unused network ports and services shall be turned off. Any network software present on CA equipment shall be necessary to the functioning of the CA application.

4.6.8 Cryptographic Module Engineering Controls

Requirements for cryptographic modules are as stated above in Section 4.6.2.

4.7 CERTIFICATE AND CRL PROFILES

4.7.1 Certificate Profile

4.7.1.1 Version Numbers

The ORC NACA shall issue version 3 certificates.

4.7.1.2 Certificate Extensions

Certificates issued by NA PKI CAs shall have the following extensions. They are:

- authorityKeyIdentifier - This extension contains the 20 byte SHA-1 hash of the binary DER encoding of the CA's public key information.
- subjectKeyIdentifier - This extension contains the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.
- keyUsage - This extension has the values of digitalSignature and nonRepudiation for signature certificates, and digitalSignature and keyEncipherment for confidentiality certificates. This extension will activated when required by consumer programs.
- certificatePolicies - This extension contains the OID listed in section 4.1.2. This extension will activated when required by consumer programs.
- basicConstraints - This extension contains the default value of CA=false. This extension will activated when required by consumer programs.

4.7.1.3 Algorithm Object Identifiers

NA PKI CAs use the sha-1WithRSA Encryption, OID {iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 29} for signatures.

CAs issue certificates using the rsaEncryption OID {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1} for identifying the algorithm the subject key was generated for:

Keys generated for use with RSA are signed using sha-1WithRSAEncryption.

4.7.1.4 Name Forms

See Section 4.3.1.1.

4.7.1.5 Name Constraints

The nameConstraints extension is not currently supported.

4.7.1.6 Certificate Policy Object Identifier

NA PKI CAs asserts the certificate policy OID identified in Section 4.1.2 of this document for certificates generated in accordance with this guideline. (Note: This must be developed yet based on the ORC OID space registration)

4.7.1.7 Usage of Policy Constraints

There are no policy constraint requirements. This extension will only be included in CA certificates when consumer programs can process it.

4.7.1.8 Policy Qualifiers Syntax and Semantics

NA PKI CAs does not include policy qualifiers in certificates.

4.7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The certificatePolicies extension is not marked critical in certificates issued by the NA PKI CAs. Agents who do not process this extension do so at risk.

4.7.2 CRL Profile

4.7.2.1 Version Numbers

NA PKI CAs shall issue version 1 CRLs exclusively. CAs shall not issue Authority Revocation Lists (ARLs) or any other partitioned CRLs.

4.7.2.2 CRL and CRL Entry Extensions

NA PKI CA certificate revocation profiles do not contain any CRL or CRL Entry Extensions.

4.8 SPECIFICATION ADMINISTRATION

This CPS is expected to remain an evolving document during its one year time period. The most current version and all official numbered drafts shall be maintained on the web site at *https://www.pki.navy.mil.*

Comments should be addressed to Mr. Bob Cope at coper@orc.com.

4.8.1 Specification Change Procedures

The NA PKI Root CAA will process any recommended changes. This CPS may be updated at any time, but draft changes shall be submitted to the .NA PKI Working Group prior to inclusion in the formal document.

4.8.2 Publication and Notification Procedures

The NA PKI Working Group shall be notified of any changes to its CPS. Notification of changes shall also be posted on the web site associated with the NA PKI operations. Subscribers shall be notified via email of any changes to subscriber obligations.

4.8.3 CPS Approval Procedures

The NA PKI Working Group will make the determination that a CPS complies with the policy identified in Section 4.1.2.

4.8.4 Waivers

The NA PKI does not meet the draft DoD Certificate Policy for Class 3 certificates in the following two areas.

4.8.4.1 FIPS 140-1 Level 2 Validated Hardware Token for CA Keys (Section 4.6.2.1)

Currently, the NA PKI is using the Netscape Certificate Authority version 1.01 software. This software does not easily permit the use of hardware tokens for storing and using CA private keys. However, NA PKI CAs will be upgraded to CMS 4.1 which, in conjunction with the nCipher, nFast/CA hardware token (key protection to FIPS 140-1 Level 2) will meet hte FIPS 140-1 Level 2 hardware token requirements for CAs.

4.8.4.2 FIPS 140-1 Level 2 Validated Hardware Token for IA Keys (Section 2.6.2.1)

Currently, IAs are using smart card tokens from DataKey. This vendor has submitted for FIPS 140-1 Level 2 validation and has passed the required cryptographic requirements. However, these cards do not yet contain the required Power On Self Test. This functionality is expected to be available by the end of calendar year 1999. IAs will migrate as soon as possible to the validated version of these tools.

5 REFERENCES

5.1 GOVERNMENT DOCUMENTS

Computer Security Act of 1987

DOD INSTRUCTION 5200.40

DOD-STD 5200.28

DoD Web Policy

Executive Order 12958

FIPS 112, Password Usage

FIPS 140-1, Security Requirements for Cryptographic Modules

FIPS 180-1, Secure Hash Algorithm

FIPS 186, Digital Signature Algorithm

Freedom of Information Act

Privacy Act of 1974

SECNAVINST 5239.3

5.2 NON-GOVERNMENT DOCUMENTS

American Bar Association Digital Signature Guidelines, dated 1 August, 1996

Internet Public Key Infrastructure X.509 Certificate and CRL Profile, dated 25 March, 1998

PKCS #11 Hardware Format

PKCS #12 Software Format

6 ACRONYMS

ACL	Access Control List
CA	Certificate Authority
CAA	Certificate Authority Administrator
COTS	Commercial Off The Shelf
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTS	Defense Travel System
EC	Electronic Commerce
EDI	Electronic Data Interchange
FAR	Federal Acquisition Regulations
FIPS	Federal Information Processing Standard
FOIA	Freedom of Information Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IA	Issuing Authority
IATO	Interim Authority to Operate
IETF	Internet Engineering Task Force
IOC	Initial Operating Capability

ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over Secure Sockets Layer
LRA	Local Registration Authority (DoD Model)
NA	Navy Acquisition
NIST	National Institute of Standards and Technology
OID	Object Identifier
OPM	Office of Personnel Management
PIN	Personal Identification Number
PKCS	Public Key Certificate Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
RA	Registration Authority
RDN	Relative Distinguished Name
S/MIME	Secure Multipurpose Internet Mail Extensions
SA	System Administrator
SBU	Sensitive But Unclassified
SSL	Secure Sockets Layer
TA	Trusted Agent
URL	Uniform Resource Locator
U.S.	United States
VPN	Virtual Private Network